Summary Description & Recommendations for Considering Data Sharing in Minnesota's Homeless Management Information System

HMIS Data Sharing

HMIS Data Sharing Workgroup

Friday November 8th, 2013

Description of HMIS Data Sharing System

PURPOSE

The HMIS Data Sharing Workgroup (the Workgroup) is pursuing options to modify Minnesota's Homeless Management Information System (HMIS) by enhancing our ability to share data among providers across the state in an effort to better serve people experiencing homelessness.

GUIDING PRINCIPLES

All considerations regarding HMIS and data sharing must seek to meet the following principles:

- Data security/privacy must be retained.
  - Pay special attention to disabilities, youth, domestic violence, etc.
  - Align with Minnesota Data Privacy Standards
- Data collection and sharing must be intentional and relevant.
- We must be clear about the "what" and "why" to be shared.
- Changes to the system must be time and cost effective.
- Any changes to the HMIS system should first consider the benefit to clients. Will the client see a difference?
  - Secondarily, we need to consider how changes will benefit providers.
- Data sharing changes to HMIS should enhance options, choices, and access for clients.
- Data sharing cannot be used as a tool to exclude individuals from services.
- We must ensure system streamlining and consistency.
- We must promote collaboration, coordination, shared goals, and a team approach.
- Consensus is not needed
  - In practice—allow for provider autonomy (option to control),
  - In planning—don't get stuck if we can't reach consensus
- We must ensure that the system is client focused.
- Make the system work for both urban and rural communities.

BACKGROUND

Over the past few years, users and funders of Minnesota's Homeless Management Information System (HMIS) have sought to determine how that system might allow greater data sharing among providers. Our current system requires individuals seeking homeless services to provide the same sensitive information at each stop, and requires each homeless service provider to input this same data into our HMIS. There are few safeguards against duplicate services or client records. HMIS reports may include inconsistencies due to these duplications. It is the Workgroup's hope that by working together and sharing data with each other, we can provide better aligned services to our customers—individuals, youth and families experiencing homelessness. We can offer better services if we know what has been tried and hasn't worked, as well as what has worked.

POTENTIAL BENEFITS OF DATA SHARING

In regions that have opened up their HMIS systems for collaborative data-sharing, providers have seen **more effective services** for the people in their programs, and **reduced duplication** in their reporting. Additionally:

- *Simplicity & Efficiency*. Alameda County, CA saw **time savings** and more effective services once they started sharing data. They initially started sharing limited data, but later opened their entire system. Michigan also saw time savings from the decreased data entry, as people only had to complete admissions once for a variety of programs. This helps people to receive the right services more quickly.
- *Improved Service Provision*. Recent Bowman System presentations demonstrated that, with data sharing, HMIS can be used as a case management tool. Michigan felt strongly that sharing data helped with **coordination of care** by allowing organizations to simultaneously build a better coordinated plan for individuals. Providers in Tampa Bay found it helpful to **see a person's story** in their service history, program entry/exits and history of changes for some data elements.
- *Improved Data Quality.* More consistent and accurate information about clients. Alameda County, CA started seeing **more relevant and accurate reports** which help with planning and funding decisions. Michigan and Tampa Bay's **accuracy of information also improved** after they started sharing data, which they attributed to providers getting to see data inconsistencies and digging for the real information.
- *Improve Communication amongst Partners*. Providers in Alameda County, CA found that sharing data **increased communication** among providers
- *Accommodate Coordinated Assessment Implementation*. A simple and efficient data system, improved service provision, trustworthy data and effective communication amongst partners are essential elements of a successful Coordinated Assessment system.
- *Improve ability to conduct system-wide analysis.* While the focus of our workgroup has remained on data sharing among providers, our workgroup has also noted the importance of enhancing regional and statewide access to data (through aggregate reports) to improve analysis of our homeless response system(s).

PROPOSED MODEL

The Workgroup worked to develop a model that honored the guiding principles identified earlier. In particular, we wanted to ensure that the model we created honored client choice. We also saw it as absolutely necessary to provide legal clarity for the system administrator, clients, agencies and funders. The following is our description of our data sharing model—including the recommendations the Workgroup is making to the HMIS Governing Group to improve Minnesota's ability to implement this model.

STEP 1: AMEND AGENCY CONTRACTS TO INDICATE PARTICIPATION IN A DATA SHARING SYSTEM

The Workgroup sought the assistance of legal data privacy experts to revise the HMIS Agency Agreement between the administrator (Wilder Research) and the end users (participating agencies). The revised Agency Agreement requires participating agencies to participate in data sharing and to adhere to data privacy standards. Michigan follows a similar model, where the HMIS administrator holds a memorandum of understanding (MOU) with all participating agencies. Like Michigan, we have developed a waiver that may release agencies[1] from their requirement to participate in data sharing. The HMIS Governing Group will identify a process to review any waiver requests that are submitted.

RECOMMENDATION

The HMIS Governing Group should adopt the revised Agency Agreement and create a waiver form to release certain agencies from data sharing participation.

[1] Providers that have the primary mission of serving survivors of domestic violence, sexual violence, and trafficking have data privacy obligations that are required by Federal Law (Violence Against Women Act—VAWA) and various funders (FVPSA, SEY, HUD, etc.) that may prohibit such providers from participating in this data sharing model. The Workgroup sees the need for further study and guidance to identify whether there are options for these organizations to participate in data sharing.

STEP 2: IDENTIFY THE AUTHORITY AND GAIN PERMISSION TO COLLECT AND SHARE DATA

Step 2 (a): Identify the authority

As the Workgroup began developing a model for data sharing, we quickly recognized that Minnesota's HMIS lacked sufficient clarity regarding which entity/entities have the legal authority to collect (much less share) data. The Workgroup enlisted the help of data privacy legal experts (state, county, administrator, provider) to address this issue. These experts identified that current Continuum of Care (CoC) regulations (2004)[2] grant the authority (to collect and share data) to any "covered homeless organization"[3]. Given the appropriate permissions, all agencies participating within HMIS have adequate authority to collect and share data.

Another option that would further simplify authority, consent and sharing would be the formation of homeless response system collaborative(s)[4]. In most regions across the country where data sharing seems to be successfully implemented, the responsibility for HMIS data sharing policy falls to one legal entity. In essence, each entity holds rights and responsibilities for determining data sharing policy that adequately meets data privacy standards. The formation of collaborative(s) will provide greater clarity regarding the entity that would have legal authority over data collection and sharing.

RECOMMENDATION
Seek legislative action to provide the authority for the formation of homeless response system collaborative(s).

It should be noted that there are some agencies that use HMIS/Bowman Systems for their homeless programs AND other program purposes/case management (i.e. free coats/clothing program). If these non-homeless programs are included within our "covered homeless organizations", it may become very cumbersome for these programs as they would need to obtain permission from each household served for the data collected. We will create a mechanism/process to ensure that agencies are able to collect and use their information for all of their programs (homeless/non-homeless) without being required to go through the higher data collection obligations for their non-homeless programs.

RECOMMENDATION
Wilder/Bowman will create separate procedures in HMIS for non-homeless programs (that will not meet the covered homeless organization definition).

Step 2 (b): Gain permission to collect and share data

The Workgroup embraced the obligation Minnesota's HMIS has in maintaining data sharing standards that fully honor the privacy of every individual in the system. We spent a considerable amount of time learning about Minnesota's and federal data privacy laws to gain a better understanding of what must be in place in order to share data.

When considering a client's consent regarding data sharing, we need to understand that there are really two separate questions/steps for seeking this consent.

Step 2 (b. i.): Permission to "collect" information. Prior to the request to share information we must obtain permission to collect information. To collect and enter data on people who are experiencing homelessness, the entity who possesses legal authority[5] must seek the consent of the client. This step may be accomplished by using a Tennessen Warning or an

[2] New Interim Regulations came out in December 2011, with a comment period that ended in February 2012. The new regulations will largely be consistent with 2004 regulations in regards to our authority questions. Regarding data sharing, it was noted that the new regulations seek to become more closely aligned with HIPAA standards (standards that our proposed data sharing model is already seeking to accommodate). Until these regulations become final, we will need to refer to 2004 Regulations for legal guidance.

[3] HUD's term for any entity participating in HMIS.

[4] See Appendix section on Collaboratives (Page 11)

[5] As noted earlier (page 2), "covered homeless organizations" have the authority to collect and share data. Covered homeless organizations are organizations that are identified within the CoC/HMIS System.

Informed Consent. We have created a HIPAA compliant form[6] that meets requirements for both Tennessen Warning and Informed Consent which will grant us permission to collect and enter data into HMIS.

- The Tennessen Warning (TW) is applicable to governmental, government-funded agencies, and agencies affiliated within a state-authorized collaborative—it is not applicable for agencies that do not receive funding from a governmental source. The TW does not require a signature and may be conducted over the phone. The TW does grant permissions to share data for purposes of coordination, payment, and administration. If all agencies entering into HMIS were government or government funded, it appears that the TW might suffice to serve as the tool to gain permission from the client to both collect and share data. Since our HMIS system currently includes a mix of both government-funded and non-government funded agencies, it is not currently possible for the TW to meet the needs for HMIS data sharing, absent legislative action to allow the formation of homeless system collaborative(s), governmental entities and non-governmental entities simply live under different requirements. For this reason, both the TW and the Informed Consent will be needed to ensure client consent has been provided to collect data for all records in HMIS.
- The Informed Consent (IC) will be needed for all agencies that do not receive government funding and are not part of a statutory collaborative. While the IC doesn't legally require a signature in all cases, we are recommending the agencies follow best practices to require a signature.
- Other items of note:
    - Again, absent of a collaborative, the purpose of the TW and IC will be limited to gathering the permission for "collecting" information, but not "sharing".
    - TW and IC forms do NOT have to list all agencies that would participate in sharing (could be listed as networks and list kept elsewhere).
    - Even if we formed a collaborative(s), HIPAA covered agencies would still need to take the additional step of obtaining a release of Information (below), to provide the exception to share protected health information.

Step 2 (b. ii.): Permission to "share" information. While the TW and IC allow us permission to collect information, a Release of Information (ROI) is needed to allow agencies to share the information that they have collected. An ROI, in essence, trumps other data privacy rules—granting permission to share data with other agencies. The ROI can be written in manner that will be HIPAA compliant.[7] The ROI will require a signature and must allow the client the option to decline.

The ROI will inform the client of active data sharing and access by all individuals approved to utilize the system. This permission allows any person working with the client to view their current and future service transactions as well as create new service transactions. The ROI has been drafted by legal experts and has been modeled off of our existing release and Dayton/Montgomery's[8] release. The ROI will expire when it is requested by the client[9]. The ROI will explain what data will be collected and shared, how it will be used, and who can access the data. The ROI includes the following:

- Data Elements to be shared[10]:

[6] Please see appendix (page 13)

[7] More information about HIPAA compliance in appendix (page 15).

[8] Please see appendix (Page 16)

[9] Under both HIPAA and the Minnesota Health Records Act, a release does not need to expire after a year. The one year expiration is a common misconception because Minnesota law provides that "[e]xcept as provided in this section, a consent is valid for one year **or** for a period specified in the consent **or** for a different period provided by law." Minn. Stat. 144.293, subd. 4 (emphasis added). Therefore, under Minnesota law, if the consent does not contain a specific expiration date, the presumption is that it expires after one year. But the law also allows a consent to contain a different expiration. Similarly, HIPAA requires an expiration date or an expiration event, but does not mandate one year. Because Minnesota law and HIPAA do not require a consent expire after one year, and a one-year expiration is very limiting, The Workgroup has opted to have the ROI expire "at the client's request". That said, best practices would be to continue to remind clients of data sharing rights and provide updated notices.

[10] Domestic violence, sexual abuse, and trafficking data will not be included in information that will be shared through this ROI.

- *Family/Household Information*
- *Income & Benefits Information*
- *Education & Employment History*
- *Housing History & Barriers*
- *Veteran Information*
- *Program & Service Involvement*
- *Health Information[11] (including physical health, HIV, & behavioral health)*

- Purposes for which data will be shared:
  - *Service Coordination*
  - *Program & Systems Development*
  - *Case Management*
  - *State-wide Evaluation*
- Entities with whom data will be shared:
  - While "share with all" will be the default option when setting up data sharing for a client, we will utilize a web-based list of organizations by "networks" which will assist clients and staff in selecting any particular agencies with whom they do not wish to share information.
- Other
  - The data sharing language in the ROI should be consistent across all providers in Minnesota.
  - The ROI might be an online screen (within HMIS) which would allow for electronic signature and/or document uploads.
  - The Workgroup strongly pursued making the ROI editable—where clients would be able to articulate what information they would be willing to share, and with whom. This approach was strongly discouraged from experts providing technical assistance for MN HMIS reform. In Michigan, they tested an editable ROI as they prepared to roll out data sharing. They found two significant problems that led them to not include this feature:
    - The editable ROI made intake much more time consuming and confusing for clients and staff. With more options, more questions and anxiety can arise.
    - Michigan's HMIS administrator and CoCs determined that an editable ROI sharply increased the likelihood of user error and data privacy breaches. Instead of working from Yes/No, providers were being asked to check many boxes in HMIS to accommodate the varying choices of clients. One miss-checked box could lead to a data privacy breach.

    It is anticipated that of all clients who are open to data sharing, very few would opt to edit their ROI. For this reason and the barriers noted above, the Workgroup has determined that we will not pursue an editable ROI. We will instead have an ROI that the clients can choose Yes/No, and will not be able to edit. It should be noted that client control regarding "What" data is shared can still be controlled by clients as they can determine this in what information they choose to give—i.e. if they don't want health information shared, they can opt not to allow that information to be collected into HMIS. Unfortunately, this option does not resolve the Workgroup's interest in allowing greater client choice regarding "Who" the information will be shared with.

RECOMMENDATION

The HMIS Governing Group will adopt new consent and release of information forms. These forms may be modified, as needed, in the future.

STEP 3: ADJUST HMIS SHARING SETTINGS TO MEET CLIENT PREFERENCES

It is of utmost importance that clients have control over their data and who has access to it. In addition, clients should be able to change their data sharing preferences over time. For example, a client entering the homeless response system may initially grant universal sharing for their data, but might later wish to limit what information is shared and with whom.

[11] There are very legitimate concerns that have warranted caution as we have considered the inclusion of health information in data sharing. Please see the appendix (page 17) to review the rationale for why the Workgroup has recommended that health information be included.

Unfortunately, Minnesota's HMIS and Bowman Systems is currently agency-centric, meaning that each agency sets its own data sharing settings for each client. Thus, if a client asked an agency to change all their data sharing settings (past, present, and future for *all* agencies); there is not currently a simple mechanism within HMIS to allow this agency to make such broad changes—each program can only control data sharing settings for data collected by their agency.

Possibilities and limitations within current HMIS system:

- *Setting sharing preferences.* Within the current system, each agency reviews the data sharing options with each client. That agency then applies the wishes of the client to the data entered in the system for their agency. Within this option, agencies can set permissions in their HMIS records for both new and historical data collected by that agency. They will not be able to set permissions for client data entered into other parts of the system (for services by other programs).
- *Changing sharing preferences.* If a client changes their mind at a later date about sharing their data, protocol will need to be put in place to differentiate between opening/closing data sharing "for one organization" and opening/closing data sharing "for client records in all of HMIS". We do not currently have a "turn on/shut off" capability in HMIS to immediately change sharing preferences system-wide. Thus, while the client can expect immediate data sharing changes from one particular agency; changes to sharing settings for all records in HMIS of this client will take more steps. This process could happen in two ways. 1) All agencies that previously entered the client's data into the system would need to manually adjust the sharing permissions to meet new client preferences; OR 2) System administrators would manually adjust sharing permissions. This will be cumbersome for both providers and the system administrator to accommodate system-wide changes in client data sharing. Efforts should be taken to make such changes as simple and quick as possible.
- *Accessing historical data.* Because the current system only allows data to be shared agency by agency, additional procedures would be needed in order to share data previously entered, especially with multiple client records entered by multiple programs.
- *Additional protocol concerns*. Client wishes to share may be different from agency wishes. With a client centric system, our desired approach would be that a client's wish to share would be more important than an agency's concerns over sharing information. It will be important to have a plan to deal with these situations if agencies choose not to share or are not allowed to share. Agency agreements, waiver forms and processes for excluding agencies when they don't meet data sharing requirements should be put in place to allow for clients to make this choice and their wishes to be followed through a set process.

RECOMMENDATION

Contract with Bowman Systems to create system rules/mechanisms that will streamline client data-sharing preference changes, including accessing historical data. In such a model, the HMIS system would apply any changes to a client's data sharing settings to all of that client's records across the system (regardless of where the records originated).

STEP 4: TAKE STEPS TO MAINTAIN AND IMPROVE DATA QUALITY

Stakeholders from across the state have expressed concerns regarding how HMIS data sharing might positively or adversely impact their data quality. In particular, providers are concerned that their reports might be altered by another provider's inaccurate data entry.

Upon initial review with Bowman Systems, it is our understanding that (while data entered by a provider will always be in the system) reports **can** be "altered" by later data entry. Some regions that have used data sharing have reported that, while some problems of altered data have occurred:

- Conflicts of altered reports and data errors have been minimal, and
- Data quality has improved overall as it has forced providers to connect and resolve data discrepancies.

RECOMMENDATION

Create the following functions/protocol to ensure data quality in an HMIS data sharing system.

HMIS System Changes

- Provider reports will be able to be drawn by "most recent entry" and by "start/end dates." Start/end date reports should provide the ability to create clean reports (drawing only/primarily from data entered by a given agency). This is a current function of HMIS.
- Work with Bowman Systems to develop new mechanisms to enhance our ability to have agency-specific reports.
- Data entry will be time-stamped and providers will be able to see who has made changes to data (and when) on a shared client. Providers do not need to see the agency/case manager name, but rather an identifier that can link the record to the person who entered the data.
- ServicePoint will have a built-in function allowing providers to send an instant message to other providers regarding data discrepancies.

HMIS Protocol Changes

- Clear protocol will be established to inform agencies how to address differences with data. A grievance policy will be in place to address unresolved issues.
- Sharing data will be a privilege, not a right. Providers that are identified to have consistently poor data quality will be restricted from utilizing data sharing. Development of standards will need to be defined prior to implementation.
- The HMIS administrator will develop a method for monitoring the impact of data sharing on data quality.
- Providers will be expected to reconcile their data in HMIS on a more frequent basis, compared to the current practice of reconciling (which vary from weekly, quarterly or annually). It was recognized that some regions (especially rural regions that have having broad geographic service regions with centralized HMIS data entry) may struggle with with new expectations for frequent data reconciliation. Technical assistance and time should be provided to help these regions adjust to recommended changes. It is also possible that expectations regarding the timeliness of data entry could be determined CoC by CoC, thus allowing greater flexibility to rural regions.

STEP 5: EQUIP CLIENTS AND AGENCIES WITH INFORMATION NEEDED TO SUCCESSFULLY IMPLEMENT DATA SHARING.

For HMIS data sharing to be successful, both clients and providers must have a clear understanding of the benefits of data sharing. Providers need to understand clearly all practices and procedures that will ensure data sharing serves the needs of those seeking help.

RECOMMENDATION

Create relevant trainings for end users that will include:

- *Communication strategies with clients*. Providers need to help the client in their decision about data sharing by specifically stating the benefits and purpose for collecting everything (this data will help me to get you the best supports), and what everything will be used for (transparency—who, what and why). Explanations to clients need to communicate that you are entering data into a network of service providers (not just the particular agency).
- *VAWA/Trauma Informed Advocacy.* Trainings should include information on how to inform and address the unique needs of people who have experienced domestic violence, sexual abuse, and trafficking when considering data sharing.
- *Understanding and navigating the network of providers available in the open HMIS system*. This training should assist providers in understanding what other agencies are participating in this open HMIS system, and how to utilize those providers in order to best serve the client's needs.
- *Required practices and protocol.* Each provider has the responsibility for ensuring that their staff is adhering to data privacy standards as outlined in agency agreements. HMIS trainings will provide clear communication to providers regarding the legal and ethical responsibilities of handling another person's personal data. Clear and

consistent consequences for substandard data use must be communicated to all end users and their organizations.

- *Minimal costs to providers*. Trainings should not lead to excessive cost/time burdens for providers.
- *Required and frequent*. Trainings are not optional. Trainings will be required of all agencies participating, in order to guarantee consistency within agencies and statewide. Trainings must be made readily available.
- *Q & A*. Trainers must be available for answering questions as they may arise for providers.

RECOMMENDATION

Continually remind clients of their data sharing rights and choices.

- Prominent signs/posters and verbal reminders should be provided at all participating HMIS agencies to remind clients of their rights regarding HMIS data sharing .

ADDITIONAL RECOMMENDATIONS TO ACCOMMODATE DATA SHARING:

- *Address end user fees*. Successful data sharing will encourage a sharp increase in end users, most of whom will need limited abilities to enter data. We need to allow this without incurring substantial costs. Affordable licensure will help ease cost burdens on agencies, and allow more people to enter information.
- *Create a system mechanism to close sharing of inactive records*. This function could be used to close child dependent records, and ensure that records collected without direct client consent would be closed until consent is provided by the individual. This function would include an ability to "unlock" expired data when a provider verifies a new Release of Information.
- *Utilize document upload function*. Data sharing provides the potential benefit to be able to expedite eligibility verification for housing, financial, disability, etc. In order to build off the verification conducted by previous providers, it will be important to be able to upload documents (homeless/housing history, disability diagnoses, financial records, etc.) so that future providers will not need to require clients to repeat documentation efforts.
- *Allow clients to retain the ability to enter as anonymous*[12]. There can be a variety of reasons (domestic violence, sexual abuse, trafficking, unaccompanied minors, etc.) why persons may choose to be entered as anonymous. At the same time, there are a variety of reasons to seek identifiable data for clients (CoC performance, ability to refer, duplication of data and time collecting data). While all clients that present will retain the right to remain anonymous, it will be important for end users to understand and communicate the value of data sharing to reduce the number of anonymous records. Anonymous clients can still choose to have their data shared by using their HMIS ID number and not their name. The HMIS ID number can be stored on a swipe-able card. MN HMIS should work with Bowman to create simple solutions to minimize duplication with anonymous users.
- *System changes and protocol to address system "searches" for client records.* The release of information—makes client data (identified in the ROI) open in the HMIS system for others in the network to "look up" or view. HMIS end users do not need to secure any further permissions to view shared client data. The Workgroup recognizes that recent data breaches in other secured systems have been the result of authorized users inappropriately accessing shared data. The Workgroup identified the following steps to provide system safeguards to ensure end users are searching for client information only as needed to serve clients better:
    - Work with Bowman Systems to create a new step on the first screen in HMIS where an end user would be reminded of their obligations regarding data use and would be required to check a box to indicate their consent to data sharing standards.

[12] Please see appendix (page 18) for description of HMIS currently operates with anonymous records.

- All end users will be trained and will be required to sign a document[13] that provides clear protocol to which all end users will adhere.
- System-wide and random audits will be conducted to identify agencies/individuals that may be searching client information beyond a "need to know" capacity.

AREAS OF CONCERN VOICED IN MINNESOTA (NOT ALREADY ADDRESSED):

- *Liability and misuse of data*. It is important for providers to know that changes in HMIS to accommodate data sharing *do not* change the liability risks for your organization. If your provider follows protocol and uses data for the purposes outlined in your agency agreement, you will not assume increased liability by participating in data sharing. However, if your organization/staff misuse client data by accessing data for purposes other than outlined in a signed ROI, you will put your agency at risk. It should be noted that this is the same risk you assume within our current system; misuse of client data puts your agency at risk. It is the expectation that all providers will be well trained and follow data privacy standards. At all times, access to the HMIS system is limited to "need to know". Internal and external auditing of use will occur[14]. Users in the HMIS system will sign an agreement to uphold all data privacy standards. Failure to adhere to sufficient standards will result in termination from the HMIS system. According to the following communities who have implemented data sharing systems (Ohio, Florida, Michigan, Delaware, and California) misuse of data has not been reported as a significant problem as they moved to an open system.
- *Scope and cost of open system*. States with open systems have found that there have been start-up costs that have incurred that have been off-set long-term with cost-savings. To address start-up costs, some regions have tied the new licensing fees to grants therefore avoiding a cost to the agency directly; other communities had the county/CoC pay for the added costs of licensing and auditing. Many states went with two different licenses – 1) data entry only and 2) data entry + reporting. There can be a fee scale for the two different types of licenses. Although a concern, the communities came up with solutions that were helpful to the agencies involved and ultimately helpful to those they serve. The Workgroup has developed a finance plan to identify possible costs and savings for the implementation of data sharing.
- *This will be more time consuming*. In communities across the country with open systems, there were definite increases in staff time during the initial startup phase (form creation, merging data, training, etc.). This did not play out as a concern over time. Once the system is up and running, agencies found clients were being served quicker, the accuracy of information was improved and data entry time was reduced. Since better data was being collected, reports were more comprehensive which impacts funding, trends, initiatives, etc.
- *It will be problematic to merge records*. Most client record will be able to merge, once shared, with minimal steps. Some client record, however, may have significant inconsistencies which may compromise our ability to immediately bring records together. Steps need to be taken to ensure records are appropriately merged.

KEY STEPS IN IMPLEMENTATION

As with any new system considering change, concerns and complications may arise in the transition that was unforeseen at the start. We cannot predict all problems, but since we are not the first community to open a system we have the wisdom of those who have gone down this road before us to provide insight. We recognize that model we describe in this document will likely look different as it moves to implementation. We strongly encourage the data sharing

[13] See *Minnesota's HMIS: User Policy, Responsibility Statement & Code of Ethics* (attached). Please contact Laura McLain (laura.mclain@wilder.org) at Wilder Research if you are not able to locate this form. In most cases, forms will be included in the distribution of this document.

[14] To make this step logistically and financially feasible, The Workgroup proposes that random sample audits take place on a monthly basis across the HMIS system.

implementation committee to maintain *flexibility* (Agile Development Methodologies) to adjust this model as needed, and to seek *simplicity* to the final system—adding complexity to the system only as it is absolutely needed.

Some suggested action steps are:

- *Hold a 30-day comment period.* Make the recommendations available on a timely basis and seek feedback from current end users, major decision makers from organizations. Information collected should be tracked by the region from which it was received.
- *Roll out data haring changes in step with HMIS TA recommendations.* HMIS technical assistance will likely lead to a number of system and protocol changes with MN HMIS. As much as possible, make all the changes at once to minimize confusion and inconsistencies.
- *Test data sharing before implementing state-wide.* The Workgroup recommends that beta and "live" testing be conducted and evaluated before implementing data sharing state-wide.
- *Meet with agency Directors/Boards across the state to fully inform agencies of changes.* Transparency and access to information will be paramount to the successful implementation of data sharing. Prior to implementation, all agency decision-makers across the state should be informed of how data sharing will impact their program.
- *Create an evaluation plan*. There are several subcategories in which to consider:
    1. Data quality / quality control (identify and track problems be it, Wilder, user or Bowman)
    2. Client satisfaction
    3. System administrator time and cost
    4. Provider time and cost
- *Identify funding during early implementation.* Search funding opportunities to cover:
    - Greater staff support for the administrator,
    - Technical solutions for Wilder/Bowman,
    - Greater overall capacity during startup,
    - New end user fees,
    - Other system capacity issues.
- *Utilize and Monitor a HMIS comment line/link.* This tool needs to be well marketed to all users to help guide the HMIS Governing group.
- *Form a Data Sharing Implementation Committee.* This group will assist Wilder with monitoring data sharing and identify solutions. This group should consist of end users and data system experts.

APPENDIX

The Rationale and Purpose of a Public / Private Collaborative

The Hearth Act and the Continuum Care (CoC) Interim Final Rule (24 CFR Part 578) codify into law the responsibility of the Continuum of Care (CoC) to develop and implement a planning process for greater coordination of a community-wide response to homelessness. They further require the CoC to develop a centralized or coordinated assessment system that will provide a comprehensive assessment of the needs of individuals and families for housing and services, and provide easy access to the most appropriate housing and services in the shortest possible time to further the goal of ending homelessness.

The Homeless Management Information System (HMIS) is a mandated system for recording personal information on persons and households in need of homeless assistance. The information collected and entered into HMIS is designed to identify the services and assistance needed by each individual to resolve homelessness and rebuild housing stability. Collectively, the information in HMIS can also inform us of community-wide needs and gaps and help us identify the most effective strategies for responding to homelessness. Historically, the HMIS has been primarily a closed system with very little data sharing between agencies because the system was designed, built and used primarily as a compliance tool for reporting aggregate data to HUD.

For Coordinated Assessment to meet the new legal requirements of efficiency and effectiveness, there must be seamless and real-time sharing of information between the agency points of contact during the assessment process and the housing and service providers to whom the homeless household members are being referred. Data sharing will eliminate the need for multiple and repetitive assessment interviews at each agency, and will allow for a continuity and consistency of service that builds on past successes and avoids the repetition of past failures.

The CoC Interim Final Rule requires the development of a coordinated assessment process as well as a comprehensive, community-wide planning effort to develop and implement the most effective possible response to homelessness. Both of those requirements underscore the need to collect, analyze and share relevant data that defines need, both for the individual and for the community. Under Minnesota state law, however, there is no clear avenue for the sharing of relevant private data between public and private agencies participating in the CoC effort.

State law does, however, currently provide for the creation of public/private collaboratives in several other areas, which allow participating government and non-profit agencies to formally organize and share information in a legal entity also recognized as a unit of government under the Minnesota Government Data Practices Act (MGDPA-- Minnesota Statues Chapter 13). One such example of this type of collaborative is the Family Services and Community-Based Collaborative authorized by Minnesota Statute 124D.23. This law allows counties, municipalities, school districts, public health entities and a variety of other community action agencies, private and non-profit service providers to integrate funding and coordinate planning and services across agencies in order to design and implement an integrated, client-centered local social service delivery system.

Because these collaboratives usually involve more than one unit of local government, they are typically organized under both the authority of the applicable collaborative statute and Minnesota Statute 471.59, which allows for the joint exercise of powers between two or more governmental units. Joint Powers Boards organized under Minnesota statute 471.59 are viewed as a “statewide entities” under the MGDPA, and are able to share data between and among the members of the entity in order to accomplish the statutory purposes of the entity.

This type of approach—a state law authorizing the creation of a CoC Collaborative-- is needed to effectively unite all of the partners in our community’s response to homelessness. We need a single, legally recognized entity that has the capacity to efficiently and effectively share all relevant information in the process of coordinating assessment and

providing housing and services to individuals and families. A legally recognized CoC Collaborative would also allow the CoC to meet the Interim Final Rules' requirements that the CoC grant applicant be a legally recognized entity, and that the CoC have a board that makes decisions for the Continuum. Our current CoC "organizations" (with "boards") are informal, are not legally recognized entities, and have no real authority or capacity to act as such.

The nature and extent of data sharing within a Continuum of Care Collaborative could be defined and limited either by a data sharing provision within the statute itself, such as exists within the Family Services and Community-Based Collaborative Statute (see, Minn. Stat. Sect. 124D.23, Subd. 5) and/or by adding provisions to the MGDPA to define "Continuum of Care data" as well as its classification, use and sharing. Any legislative approach should allow the sharing of data between and among collaborative members, but only on an as needed/minimum necessary basis, while also providing the usual high level of privacy protection for private or confidential data both within and outside of the operations of the Continuum of Care.

Any statutory CoC collaborative authority should also allow local units of government to organize CoC's flexibly, as needed, on a local, regional or state-wide basis. This type of approach, in conjunction with a heightened ability to share information, would facilitate our capacity to be in compliance with the requirements of the Hearth Act and the CoC Interim Final Rule, significantly improve our ability to respond effectively to homelessness, and develop meaningful plans for the on-going improvement and implementation of our Continuum of care.

It is important to stress that creating a legislatively approved CoC collaborative would not alter the right of the individuals to exercise control over their personal and private data. While the careful and judicious sharing of information for the purpose of providing services and assistance can improve the efficiency and effectiveness of those services, it would remain fully within the control of the individual to determine whether and what information can be shared and with whom. In the context of a legislatively authorized CoC collaborative, no individual would be asked to supply private or confidential data without initially being informed of: the purpose and intended use of the requested data; whether the individual may refuse or is legally required to supply the requested data; any known consequences arising from supplying or refusing to supply private or confidential data, and; the identity of other persons or entities authorized by state or federal law to receive the data. This required notification, embodied in the "Tennessen Warning" under state law and the "Notice of Privacy Practices" under federal law (HIPAA), would always be provided to any prospective CoC client before any data is initially requested and collected, and would allow the CoC client to control the nature and extent of their information disclosure.

New Consent and Release of Information forms[15]

Background

Minnesota's Homeless Management Information System (HMIS) is a database used by programs that offer services aimed at limiting or eliminating homelessness. The U.S. Department of Housing and Urban Development (HUD) requires local jurisdictions to implement locally-controlled HMIS systems in order to compete for substantial annual funds it provides for purposes of housing those experiencing homelessness. In Minnesota, the HMIS is a statewide system managed by Wilder Research, which serves as the required data collection and reporting tool for several federal and state funding streams. Over 200 service-providing agencies ("Participating Agencies") routinely enter data into Minnesota's HMIS about the clients they serve.[16]

Wilder Research ("Wilder"), a division of the Amherst H. Wilder Foundation administers Minnesota's HMIS, including project coordination, training and consultation, and database management. The project is funded from a number of private and public sources, pursuant to a number of contracts and Grant Agreements. For example, the Minnesota Housing Finance Agency ("MHFA") contracts with Wilder to administer HMIS for the Family Homeless Prevention Program. Additionally, Wilder receives grant money directly from HUD to subsidize its administration of HMIS.

In 2004, HUD released its final rule for HMIS Data and Technical Standards.[17] The regulations broadly allow a Covered Homeless Organization ("CHO") (also referred to in this memorandum as Participating Agencies) to use and disclose protected personal information (PPI) from an HMIS to (1) 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. There are additional permissive use and disclosure standards, which include uses to avert a serious threat to health or safety, uses for academic research purposes, and disclosures for law enforcement purposes.

On December 5, 2011, HUD released new proposed HMIS regulations pursuant to the HEARTH Act. The proposed rule generally relates to uniform technical requirements, proper collection and maintenance of the database, and confidentiality of the information in the database. The comment period on the proposed rule closed on February 7, 2012. However, to date HUD has not published a final rule. Until the final rule is published, HMISs that are currently in operation should continue to use the standards under the 2004 Technical Standards.

Workgroup Plan

Stakeholders in Minnesota established the HMIS Data Sharing Workgroup ("Workgroup") to review and modify the current HMIS model to enhance the ability to share data among HMIS Agencies across the state to better serve people experiencing homelessness. The Workgroup identified several concerns regarding the legal authority for enhanced data sharing:

- HMIS Agencies that are Covered Entities under HIPAA cannot share data absent patient authorization.
- HMIS Agencies that are part of state government, or under contract with a state governmental body, are required to abide by the Minnesota Government Data Practices Act with respect to use and sharing of information.
- HMIS Agencies that are part of state government which collect data from individuals must provide individuals with the Tennessen Warning, which lists which agencies may view the data.

[15] Please contact Laura McLain (laura.mclain@wilder.org) at Wilder Research if you are not able to locate the new forms. In most cases, forms will be included in the distribution of this document.

[16] Minnesota's HMIS relies on software provided by Bowman Systems, called ServicePoint. Some agencies that participate in Minnesota's HMIS also use ServicePoint to track other services that are not directly relevant to HMIS. These other services are NOT considered part of Minnesota's HMIS; this memo does not speak to use of ServicePoint for non-HMIS purposes.

[17] Federal Register, Vol. 69, No. 146, July 30, 2004

- Existing Agency Agreements between HMIS Agencies and Wilder contain a provision allowing the HMIS Agency to wholly opt-in or opt-out of data sharing with other providers. If the agency opted-out in the agreement, Wilder cannot broadly share the information.
- Not all Participating Agencies are part of state government.

In response to these concerns, the Workgroup developed a new approach to data sharing.

- The New Agency Agreement template between Wilder and an HMIS Agency no longer contains a provision allowing the provider to wholly opt-in or opt-out of data sharing. Instead, under the new model, individuals will determine whether their information can (1) be entered into the HMIS and (2) be shared by HMIS/Wilder with the other HMIS Agencies. This is a two-step approach.
- **Step One – Minnesota's HMIS Data Privacy Notice & Consent to Enter Information Into HMIS.**
    - This form allows an HMIS Agency to collect and enter client information into HMIS.
    - If only this form is signed, the information can be entered into the system but cannot be broadly accessed by other HMIS Agencies.
    - However, the information can be seen and used for HMIS purposes. It can be seen by people outlined in the form, including the people who work for the provider, auditors or funders (including HUD where applicable), Wilder, for research purposes, and for other limited purposes.
    - This form is HIPAA-compliant, therefore the information may be entered by Covered Entities.
    - For Covered Entities subject to HIPAA, the form must be signed.
    - For non-Covered Entities, best practices is a signed form, but where a signed form is not feasible, verbal notice and consent is acceptable.
    - For purposes of data related to HMIS, the form also constitutes a Tennessen Warning and authorization to share information under the Minnesota Government Data Practices Act
- **Step Two – Minnesota's HMIS Release of Information**
    - This form allows an individual to choose whether or not to have information shared with other HMIS providers.
    - Even if an individual chooses not to have information shared with other HMIS Agencies, the information may still be shared with the limited individuals listed on the Data Privacy Notice & Consent to Enter Information Into HMIS form. Under federal regulation, the information can always be shared with these individuals (except for Covered Entities under HIPAA which require a signed authorization to enter the information).
    - This form is HIPAA-compliant, therefore the information may be entered by Covered Entities.
    - For Covered Entities subject to HIPAA, the form must be signed.
    - For non-Covered Entities, best practices is a signed form, but where a signed form is not feasible, verbal notice and consent is acceptable.
    - The form also constitutes a Tennessen Warning and authorization to share information under the Minnesota Government Data Practices Act, so for government agencies, this form should be signed.
- HMIS Participating Agencies that wish to be excluded from data sharing on an agency-wide basis, such as domestic violence agencies, chemical dependency programs, or youth agencies may complete a Data Sharing Requirement Waiver Request.

HIPAA

The Workgroup understands the obligations of many providers within HMIS to adhere to the data privacy standards within HIPAA. It was understood that our HMIS Data Sharing model would need to either accommodate the compliance needs for HIPAA organizations or would need to exempt such organizations from participating in a data sharing system. With the consultation of state, county, administrator and provider data privacy experts; we are very confident that we have created a data sharing model that is fully HIPAA-compliant and will thus allow all HIPAA covered organizations to participate in data sharing.

Data Privacy experts made a few of observations that will be helpful for the reader:

- *Who is a HIPAA covered organization?* Most organizations that collect health information think that they are HIPAA covered, but in fact, many are not. In fairness to these organizations, there are a lot of grey areas. Protected health information is covered by HIPAA when you are one of the following "covered entities":
    - Health Plan
    - Health Care Clearinghouse
    - Health Care Provider

  HIPAA allows these covered entities to use protected information for:
    - Treatment
    - Payment
    - Health Care Operations

  If you are not one of these entities it does not mean that just because you have health info that it is HIPAA covered. Organizations will often just assume all health information must be HIPAA compliant due to the fear of the Office of Inspector General (OIG)—enforcement entity, when they are not. Some organizations are a hybrid (not everything they do is HIPAA covered, but some of the programs/services they provide are HIPPA "covered" functions), and therefore may be obligated to meet HIPAA standards for particular programs /services.

- *How can HIPAA organizations share protected health information?* There are ways for HIPAA covered agencies to share protected health information with non-covered entities in certain circumstances when an exception is granted by HIPAA and the disclosure is authorized by some other state or federal law (see section 512 disclosures, 45 CFR Section 164.512). HIPAA standards require that organizations are prohibited from sharing Protected Health Information (PHI) UNLESS they have an authorization or have an exception. **Authorization can be the RELEASE OF INFORMATION**. The MN HMIS Release of Information has been designed to be HIPAA compliant.

- *What are HIPAA organizations allowed to share without a release of information?* Without the release of information noted above, HIPAA organizations (not sharing protected health information) can still share basic identifiers.

Dayton/Montgomery's Release of Information Model

EXHIBIT B

Dayton-Montgomery County HMIS Client Notice and Consent for Release

I, _____ (insert client's name), understand that _____ ("Agency") is a partner agency in the Homeless Management Information System (HMIS). I authorize the collection of information about the services provided to me by the Agency and for this information to be included in the HMIS database, which shall be used by the Agency and Montgomery County to improve services to me and the services offered to others.

By initialing the "yes" below, I agree that information in the HMIS will be shared with other agencies. A description of the information shared and the partner agencies in the HMIS is listed below. The agencies that participate in the HMIS may change from time to time. A copy of the current list of agencies is available upon request.

Yes: _____ No: _____

Date: _____ Signature: _____

DESCRIPTION OF INFORMATION THAT IS SHARED

The Dayton-Montgomery County HMIS Client Release Form authorizes the following identifying information to be routinely shared using the Dayton-Montgomery County HMIS to better help me and/or my family.

Assessment Information Related to:

- Family/Household Information
- Income and Benefits Information
- Education and Employment History
- Housing History and Barriers
- Veteran Information
- Program and Service Involvement
- Health Information, including physical health, HIV, behavioral health

LIST OF PARTICIPATING HOMELESS ORGANIZATIONS

AIDS Resource Center Ohio
Daybreak
Holt Street Miracle Center
Homefull
Homeless Solutions (Montgomery County)
Goodwill Easter Seals Miami Valley
Linda Vista
Mercy Manor
Miami Valley Housing Opportunities
PLACES
Red Cross Dayton Chapter
St. Vincent de Paul
Samaritan Homeless Clinic
VA Medical Center
Volunteers of America
YWCA Dayton

Line through and initial any agencies in the above list with whom you do **not** want to share information.

Rationale for Sharing Personal Health Information in HMIS

The law provides the individual the absolute right to protect personal information that is collected by any agency for the purpose of defining need and designing services to meet that need. This is particularly true of private health information, given the potential harm that unwarranted disclosure can have.

The case for the careful, judicious sharing of private health information through a secure, on-line database such as HMIS need not, in any way, conflict with the legal protections provided to the individual to control who might have access to this information.

No information may be entered into HMIS without the expressed consent of the individual and a bedrock principle for our HMIS system since the beginning, is that no services may be denied solely because of a person's denial to have information entered into the system.

Even if information is entered into the system, the individual has the right to require that none of that information, or only some of that information can be shared with other agencies, and the right to specify agencies who may and who may not have access. And, furthermore, the individual has the right to change that decision to share, or not share, at any time.

The purpose of collecting private health information in the first place is done for several reasons, including:

- To determine grounds for eligibility for specific services and assistance (i.e., when a disability diagnosis is required for eligibility).
- To align those services with health and medical needs.
- To determine, for purposes of referral and plan development, the specific needs that will need to be met, and the types of expertise required to meet those needs.

The argument for sharing that information securely to others, and only for the purpose of providing services consistent with needs that may be dictated by one's health situation, is exactly the same as the arguments for collecting the information in the first place, plus another very important consideration.

It may seem that denying access to one's private health information through HMIS is a way to make the system less intrusive, but, in fact, can very well be the opposite. Revealing one's private health information to a stranger can be a difficult and, at times, humiliating experience. If that experience has to be repeated at every agency in order to access services, this, in itself, might be a significant disincentive to seeking the help that is needed. When that information is available securely through HMIS to others attempting to provide assistance, the need to repeatedly rehash that information can be significantly reduced.

Sharing data securely, including private health information, enables each service stop along the person's journey from homelessness to stability to build on previous successes and avoid repeated failure. It can promote a more seamless system of assistance from one provider to the next, and it can do so while also being less aggressively intrusive into, and, at the same time, more respectful of the individual's right to privacy.

Anonymous Client Process (How HMIS currently operates with anonymous records)

When client information is entered into the system, whether anonymous or not, that record is assigned a unique system ID number. Clients can be looked up based on this ID, or searching for their name, social security number or alias (which can be anything the user would like to enter such as an agency ID).

When clients choose not to have their identifying information entered into the system, there is an option to enter the information as "Anonymous." There is a separate initial client creation button called: Add as Anonymous. This button systematically adds a first name of "Anonymous" and a last name starting with ZZ then a series of numbers that includes the client ID. We recommend that Social Security number not be added if a client chooses to be anonymous since this information can be identified by others and is specific to the client. Other demographic information can be entered as long as the client chooses to.

This system ID number is the only distinguishing item from other anonymous records in the system. Users should write down the client's system ID number in order to be able to look up their record again. We recommend that user keep this number in the client's file or another tracking document of anonymous clients.

The first and last name fields, along with other identifying information such as Social Security number, can still be edited to record the client's information if the client changes their mind. If a client wishes to have their identifying information removed from the system and become anonymous; users can contact Wilder staff to assist with this process since there is no current way to modify that at the end user level without deleting the current record and reentering as anonymous. More on the "Alias" field: This is an optional field. It can be used to record any information to find the client that the user finds helpful. It is important with an anonymous client that no identifying information such as initials or nickname is recorded. An agency client ID or other tracking number may be most useful for helping to have another method for identifying and searching for an anonymous client record.

Cost Projections

Costs associated with changing the data security model of Minnesota's HMIS *to enable more efficient services-provision and better align with coodinated assessement*		
PLEASE NOTE: These costs are estimates and may not account for all costs or savings that will result in HMIS Data Sharing implementation.		
Item	**Estimated Cost**	**Notes**
Policy development (calendar 2013, including meetings, research, legal fees)	**$20,000**	*System admin costs only; absorbed within existing HMIS "Main Trunk" budget, per Governing Group directive*
Development and initial implementation (Year 1: calendar 2014)		
System Admin (Wilder Research with assistance from Bowman Systems)	**$44,000**	*These costs may be covered by new HMIS/ SHP grants, pending Governing Group approval.*
Planning and testing (developing ServicePoint set-up to correspond with changes)	*$7,000*	
Implementing system changes in ServicePoint	*$5,000*	
Developing instruction documents	*$1,500*	
Developing training procedures & curriculum	*$4,000*	
Providing Training (including in-person; webinars; and user groups as needed)	*$7,500*	
Monitoring & troubleshooting, including record merging	*$8,000*	
Translation of privacy forms (Spanish, Somali, Hmong)	*$3,000*	
Potential costs for service-providing agencies participating in HMIS		*These costs likely would need to be covered by resources internal to the agencies participating in HMIS*
Attending Initial Training	2 hrs/user if done remotely, 4 hrs (with some travel time) if in person	
Discussing Data sharing with clients and completing forms	10-15 minutes/client	
Additional data entry steps and troubleshooting	2-15 minutes/client	
Additional end-user licenses[18]	Currently $250/ license + $50 initial training fee	
Potential On-going annual costs (above and beyond current costs; Calendar 2014 and beyond)		
System Admin (Wilder Research with assistance from Bowman Systems)	**$16,500**	
Maintaining and improving instructional documents	$0	*Same as current*
Annual privacy training: Updating, delivering, tracking	$6,500	
Additional end-user support	$6,000	
Monitoring & troubleshooting, including record merging	$4,000	

[18] This is an annual cost.

Service-providing agencies participating in HMIS		
Attending yearly training	2 hours per user if done remotely	
Discussing Data sharing with clients and completing forms	10-15 minutes per client	
Additional data entry steps and troubleshooting	2-15 minutes per client	
Additional end-user licenses	Currently $250/ license + $50 initial training fee	

Other possible related costs		
Moving to real-time data entry		
Wilder Research and/or Bowman Systems consultation to support the incorporation of real-time data entry into business practices of individual organizations	$1,200+ per organization (?)	
Adaptation to new business process within each agency	Unknown	*Could be net gains in efficiency over time; likely a sizable time investment in initial roll-out.*
Additional User Licenses: System-wide, aggregate costs[19]		
2 additional per agency (500 total) at current costs ($250 per)	$125,000	
3 additional per agency (750 total) at current costs ($250 per)	$187,500	
Mobile Technology (smartphones , tablets)	Unknown	
Bowman Costs		
Changing to client centric data entry model with ability to open/close all records in system at once	Unknown	
Instant messaging within system to contact users about data questions	Unknown	

[19] Annual costs