Community Wide HMIS
Access – Privacy and Security Plan

All records entered into the HMIS are downloaded from HMIS and are required to be kept in a confidential and secure manner.

Oversight:

1) All Agency Administrators with support of agency Leadership must:
    a. Insures that all staff using the system complete annual privacy and security training. Training must be provided by MSHMIS Certified Trainers and based on the MSHMIS Privacy/Security Training Curriculums.
    b. Conducts quarterly review of their Providers Visibility insuring that it properly reflects any signed Sharing QSOBAAs, their adapted Release of Information, and the privacy script used to explain privacy for all clients.
    c. Insures the removal of licenses to HMIS when a staff person leaves the organization or revision of the user's access level as job responsibilities change.
    d. Reports any security or privacy incidents to the local lead HMIS System Administrator for the CoC jurisdiction. The System Administrator investigates the incident including running applicable audit reports. If the System Administrator and Security Officer determine that a breach has occurred and/or the staff involved violated privacy or security guidelines, the System Administrator will report to the chair of the CoC. A corrective action plan will be implemented. Components of the plan must include at minimum supervision and retraining. It may also include the removal of the HMIS license, client notification if a breach has occurred, and any appropriate legal action.
2) Criminal background checks must be completed on all Local System Administrators by the Local Lead Agency. All agencies should be aware of the risks associated with any person given access to the system and limit access as necessary. System access levels should be used to support this activity.
3) The HMIS Lead Agency conducts routine audits of participating agencies to insure compliance with the Operating Policies and Procedures. The audit will include a mix of system and on-site reviews. The Lead Agency documents the inspection and recommendations.

Privacy:

1) All agencies are required to have **HUD Privacy Notice** posted and visible to clients where information is collected.
2) All agencies must have a **Privacy Notice**. They may adopt the MSHMIS sample notice or integrate MSHMIS into their existing notice. All privacy notices must define the use and disclosures of data collected on MSHMIS including:
    a. The purpose for the collection of client information.
    b. A brief description of policies and procedures governing privacy including protections for vulnerable populations.

c. Data collection, use and purpose limitations. The uses of data must include de-identified data.
d. The client's right to copy/inspect/correct their record. Agencies may establish reasonable norms for the time and cost related to producing any copy from a record. The agency may say "no" to a request to correct information, but the agency must inform the client of its reasoning within 60 days of the request.
e. The client complaint procedure.
    i. Client's that are unhappy about the data collection process or feel their data has been compromised may complain directly to the Director of the CoC. Complaints will be reviewed monthly with MCAH.
        1. Step 1: Send an email or submit a paper complaint to the Director of the CoC.
            a. Email is nad@summitpointe.org or drop-off/mail to CoC/Summit Pointe, 140 W. Michigan Ave., Battle Creek, MI 49017
            b. If the client prefers to send an email but has no access to a computer, staff at Summit Pointe Housing will assist with the process.
        2. Step 2: The complaint will be discussed with MCAH.
        3. Step 3: After deliberations, an email or paper letter will be generated from the CoC explaining the resolution or next steps if required.
f. Notice to the customer that the privacy notice may be updated overtime and applies to all client information held by the agency.

3) All notices will be compiled at the CoC level and the HARA for Calhoun County.
4) All agencies are required to have a **Privacy Policy**. The privacy policy must include:
    a. Procedures defined in the agencies privacy notice.
    b. Protections afford those with increased privacy risks such as protections for victims of domestic violence, dating violence, sexual assault, and stalking. Protection included at minimum:
        i. Closing of the profile search screen so that only the serving agency may see the record.
        ii. The right to refuse sharing if the agency has established an external sharing plan.
        iii. The right to be entered under an un-named record protocol where identifying information is not recorded in the system and the record is located through a randomly generated number (note: this interface does allow for un-duplication because the components of the unique client ID are generated).
    c. Security of hard copy files:
        i. Agencies may create a paper record by printing the assessment screens located within HMIS. These records must be kept in accordance with the procedures that govern all hard copy information (see below).
    d. Client information storage and disposal:
        i. Users may not store information from the system on personal portable storage devices.
        ii. The agency will retain the client record for a period of seven (7) years, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised.
    e. Remote access and usage:

i. The agency must establish a policy that governs the use of the system when access is approved from remote locations. This policy must address:
    1. The use of portable storage devices with client identifying information is strictly controlled.
    2. The environments where use is approved are not open to public access and all paper and electronic records that include client identified information are secured in locked spaces or are password controlled.
    3. All browsers used to connect to the system must be secure. **No user is allowed to access the database from a public or non-secured private network such as an airport, hotel, library, or internet café.**
    4. All computers that access the system are owned by the agency.

5) Agencies must protect **hard copy data** that includes client identifying information from unauthorized viewing or access.
    a. Client files are locked in a drawer/file cabinet.
    b. Offices that contain files are locked when not occupied.
    c. Files are not left visible for unauthorized individuals.
6) Agencies provides a **Privacy Script** to all staff charged with explaining privacy to standardize the explanation of agency privacy rules. The script must:
    a. Be developed by the agency leadership to reflect the agencies sharing agreements and the level of risk associated with the type of data the agency collects and shares.
    b. The script should be appropriate to the general education/literacy level of the agencies clients.
    c. A copy of the script should be available to clients as they complete the intake interview.
7) Agencies that plan to share information through the system must sign a Sharing QSOBAA. The sharing agreement is implemented with the following information:
    a. The agreement prescribes the re-release of information shared under the terms of the agreement.
    b. The agreement specifies what is shared and with whom.
    c. Agencies may share different things with different community partners and may sign multiple Sharing QSOBAAs to define the layered practice.
    d. The signatories on the agreement include authorized representatives from all agencies covered by the agreement.
    e. All members of the Sharing QSOBAA are informed that by sharing the electronic record they are creating a common record that can impact the data reflected on reports. Members of the sharing group agree to negotiate data conflicts.
    f. No agency may be added to the agreement without approval of all other participating agencies.
        i. Documentation of that approval must be available for review and may include such items as meeting minutes, email responses, or other written documentation.
    g. When a new member is added to the Sharing QSOBAA, the related visibility group is end-dated and a new visibility group has begun. **A new member may not be added to an existing visibility group.**
8) Agencies must have an appropriate **Release(s) of Information (ROI)** that are consistent with the type of data the agency plans to share.
    a. The agency has adopted the MSHMIS basic Release of Information appropriate to their sharing practice to share basic demographic and transaction information.

b. If the agency integrates the MSHMIS release into their existing releases, the release must include the following components:
    i. A brief description of MSHMIS including a summary of the HUD public notice.
    ii. A specific description of the client profile search screen and an opportunity for the client to request that the screen be closed.
    iii. A description of the agencies sharing partners (if any) and a description of what is shared, and must reflect term of the agreement.
    iv. A defined term of the agreement.
    v. Inter-agency sharing must be accompanied by the negotiations of a Sharing QSOBAA.
c. A HIPAA complaint **Authorization to Release Confidential Information** is also required if the planned sharing includes any of the following:
    i. Progress notes.
    ii. Information or referral for health, mental health, HIV/AIDS, substance abuse, or domestic violence.
    iii. To streamline paper, the basic HMIS release may be adapted to include the language necessary for a HIPAA complaint release of sharing practice is likely to include the items above in ii.

9) An **automated ROI** is required to enable the sharing of any particular client's information between any Provider Pages on the system.
    a. Agencies should establish internal sharing by creating a Visibility Group(s) that includes all agency provider pages where sharing is planned and allowed by law.
        i. **Internal sharing** does not require a client release of information unless otherwise specified by law.
        ii. If provider pages are added to the agency tree, they may be included in the existing visibility group. The information available to that provider page will include all information covered by the visibility group from the beginning date of the group – sharing will be retrospective.
    b. Agencies may elected to share information with other agencies – **External Sharing** – by negotiating a Sharing QSOBAA (see seven (7) above).
        i. A signed and dated client release of information(s) must be stored in the client record (paper or scanned onto the system) for all automated ROIs that release data between different agencies – external sharing.
        ii. To prevent retrospective sharing a new visibility group is constructed whenever a new sharing partner is added to the agencies existing sharing plan/QSOBAA.
10) The agency must have a procedure to assist clients that are hearing impaired or do not speak English as a primary language. For example:
    a. **Agencies are required to maintain a culture that supports privacy.**
        i. Staff do not discuss client information in the presence of others with a need to know.
        ii. Staff eliminate unique client identifiers before releasing data to the public.
        iii. The agency configures workspaces for intake that supports privacy of client information and data entry.
        iv. User accounts and passwords are not shared between users or visible for others to see.

v. Project staff are educated to not save reports with client identifying data on portable media as evidenced through written training procedures or meeting minutes.
vi. Staff are trained regarding use of email communication.

11) All staff using the system must complete privacy and security training annually. Certificates documenting completion of training must be stored for review upon audit.
12) Victim Services Providers are precluded from entering client level data on the HMIS or providing client identified data to the HMIS. These providers will maintain a comparable database to respond to the grant contract.

Data Security:

1) All licensed users of the system must be assigned **access levels** that are consistent with their job responsibilities and their businesses "need to know".
2) All computers have **virus protection with automatic updates**.
    a. Agency Administrators or designated staff are responsible for monitoring all computers that connect to the HMIS to insure:
        i. The anti-virus software is using the up-do-date virus database.
        ii. The updates are automatic.
        iii. OS updates are also run regularly.
3) All computers are protected by a Firewall.
    a. Agency Administrators or designated staff are responsible for monitoring all computers that connect to the HMIS to insure:
        i. For single computers, the software and version is current.
        ii. For network computers, the firewall model and version is current.
        iii. That updates are automatic.
4) Physical access to computers that connect to the HMIS is controlled.
    a. All workstations are in secured locations (locked offices).
    b. Workstations are logged off when not manned.
    c. All workstations are password protected.
    d. **All HMIS users are prescribed from using a computer that is available to the public or from access to the system from a public location through an internet connection that is not secured**. That is staff are not allowed to use internet cafes, libraries, airport Wi-Fi, or other non-secure internet connections.
5) A plan for remote access if staff will be using HMIS outside of the office such as doing entry from home. Concerns addressed in this plan should include the privacy surrounding of the off-site entry.
    a. The computer and environment of entry must meet all of the standards defined above.
    b. Downloads from the computer may not include client identifying information.
    c. Staff must use an agency-owned computer.
    d. System access settings should reflect the job responsibilities of the person using the system. Certain access levels do now allow for downloads.

Remember that your information security is never better than the trustworthiness of the staff you license to use the system. The data at risk is your own and that of your sharing partners. If an

accidental or purposeful breach occurs, you are required to notify M.C.A.H. A full accounting of access to the record can be completed.

Disaster Recovery Plan:

The HMIS can be a critically important tool in the response to catastrophic events. The HMIS data is housed in a secure sever bank in Shreveport, LA with nightly off-site backup. The solution means that data is immediately available via the Internet connection if the catastrophe is in Michigan and can be restored within four (4) hours if the catastrophe is in Louisiana.

1) HMIS Data System (see "Bowman System Securing Client Data" for a detailed description of data security and Bowman's Disaster Response Plan):
    a. MSHMIS is required to maintain the highest level disaster recovery service by contract with Mediware for Premium Disaster Recovery that includes:
        i. Off-site, out-of-state, on a different Internet provider and on a separate electrical grid backups of the application server via a secured Virtual Private Network (VPN) connection.
        ii. Near-Instantaneous backups of application site (no files other than five (5) minutes).
        iii. Nightly off-site replication of the database in case of a primary data center failure.
        iv. Priority level response (ensures downtime will not exceed four (4) hours).
2) HMIS Lead Agencies:
    a. The local System Administrator will continuously be in communication with MCAH in regards to the back-up of data done by Mediware.
3) Communication between the staff of the Lead Agency, the CoC, and the agencies in the event of a disaster is a shared responsibility and will be based on location and the type of disaster.
    a. Agency Emergency Protocols must include:
        i. Emergency contact information including the names, organizations, and phone numbers of local responders and key internal organizational staff, a designated representative of the CoC, the local HMIS lead agency, and the MSHMIS Project Director.
        ii. Persons responsible for the notification and the timeline of the notification.
    b. In the event of a system failure:
4) Mediware will inform MCAH if there is a system failure. MCAH will inform local SA1 who will then inform their local agencies and end users. In this case we would inform local leadership and all agencies and end users. We do this via email and if necessary phone calls.
        i. After business hours, MSHMIS staff report system failures to Mediware using the emergency contact protocol. An email is also launched to local System Administrators and Emergency Shelter designated staff no later than one hour following the identification of a failure.
    b. MSHMIS Project Director or designated staff will notify the HMIS Vendor if additional database services are required.
5) In the event of a local disaster:
    a. MSHMIS in partnership with the local lead agency will provide access to additional hardware and user licenses to allow the CHO(s) to reconnect to the database as soon as possible.

b. MSHMIS in collaboration with the local lead agencies will also provide information to local responders as required by law and within best practice guidelines.
c. MSHMIS in collaboration with the local lead agencies will also provide access to organizations charged with crisis response within the privacy guidelines of the system and allowed by law.

Data Quality Plan:

1) Agencies must require documentation at intake of the homeless status of consumers according to the reporting and eligibility guidelines issued by HUD. The "order of priority" for obtaining evidence of homeless status are:
2) 100% of the clients must be entered into the system within 15 days of data collection. If the information is not entered on the same day it is collected, the agency must assure that the date associated with the information is the date on which the data was collected by:
    a. Entering the entry/exit data including the UDEs on the entry/exit tab of ServicePoint or
    b. Backdating the information into the system:
        i. Written instructions for backdating information in the system can be found on MCAH job aids. End users need to backdate to the date the information was collected by the client.
3) All staff are required to be trained on the definition of homelessness.
    a. MSHMIS provides a Homeless Definition Cross-Walk to support agency level training.
    b. Documentation of training must be available for audit.
    c. There is congruity between the following MSHMIS case record responses, based on the applicable homeless definition (housing status and residence prior to entry are being properly completed).
4) Agencies have a process to ensure that first and last names are spelled properly and the DOB is accurate.
    a. An ID is required at intake to support proper spelling of the client's name as well as the recording of the DOB.
    b. If no ID is available, staff request the legal spelling of the person's name. **Staff should not assume they know the spelling of the name**.
    c. Projects that serve the chronic and higher risk populations are encouraged to use the Scan Card process within ServicePoint to improve un-duplication and to improve the efficiency of recording services.
    d. Data for clients with significant privacy needs may be entered under the "Un-Named Record" feature of the system. However, while identifiers are not stored using this feature, great care should be taken in creating the un-named algorithm by carefully entering the first and last name and the DOB. Names and ServicePoint ID numbers Cross-Walks (that are required to find the record again) must be maintained off-line in a secure location.
5) Income and non-cash benefits are being updated at least annually and at exit.
    a. For PH projects with long stays, at the annual review, income over two (2) years old must be updated by closing the existing income and entering a new record (even if the income has not changed). This assures that the income has been reconfirmed.

b. For all other projects, any income(s) no longer available to the client should be closed at intake (shared data from another provider), annual review and exit. If the income is over two (2) years old, please follow the procedure defined above.

6) Agencies have an organized exit process that includes:
    a. Clients and staff are educated on the importance of planning and communicating regarding discharge. This is evidenced through staff meeting minutes or other training logs and records.
    b. Discharge destinations are properly mapped to the HUD destination categories.
        i. MSHMIS provides a destination document to support proper completion of exits.
    c. There is a procedure for communicating exit information to the person responsible for data entry if not entering real name.
7) Agency Administrator/Staff regularly run data quality reports.
    a. Report frequency should reflect the volume of data entered into the system. Frequency for funded projects will be governed by grant agreements, HUD reporting cycles, and the CoC standards. However, higher volume projects such as shelters and services only projects must review and correct data at least monthly. Lower volume projects such as transitional and permanent housing must run following all intakes and exits, and quarterly to monitor the recording of services and other required data elements including annual updates of income and employment.
    b. The project entry and exit dates should be recorded upon project entry and exit of all participants. Entry dates should record the first day of service or project entry with a new project entry date for each period/episode of service. Exit dates should record the last day of residence before the participant leaves the shelter/housing project or the last day a service was provided.
    c. Data quality screening and correction activities must include the following:
        i. Missing or inaccurate information in red Universal Data Element fields.
            1. The relationship to household assessment question is completed.
            2. The client location question is completed.
            3. Time on streets, in shelter, or safe haven is completed included the revised 2015 homeless history chronic question series is properly completed.
        ii. All project specific required fields are completed. Of special interest:
            1. The status of domestic violence flight is completed (new question).
            2. HUD verifications are completed on all income, non-cash benefits, insurance, and disability sub-assessments are completed.
            3. The residential move-in-date is completed for all PH-RRH projects.
        iii. Un-exited clients using the Length of Stay and Un-Exited Client Data Quality reports.
        iv. Provider Page Completion Reports with an annual update of the HUD Data Standard Elements.
            1. The Federal Partner Funding Source is completed with “NA” if no Federal funding sources exist or the name of the Federal Partner, grant number and grant dates are completed.
            2. New CoC sub-assessments is completed and aged-out pages are identified via page naming and CoC code convention.
            3. The primary provider contact information reflects where the services are being delivered.

4. Close all inactive provider pages using the naming protocol. Audit of inactive pages includes closing all open services, incomes, and exiting all un-exited clients.

8) The CoC and agencies are required to review outcome performance reports defined by HUD and other funding organizations. Measures are adjusted by project type. The CoC Lead Agency, in collaboration with the CoC Reports Committee or other designated CQI Committee, establishes local benchmark targets for performance improvement on shared measures.
9) MSHMIS publishes regional benchmarks on all defined measures annually.
10) Agencies are expected to participate in the CoC's Continuous Data Quality Improvement Plan.

Electronic Data Exchange:

1) Agencies electing to either import or export data from the MSHMIS must assure:
    a. The quality of data being loaded onto the system meets all the data quality standards listed in this policy including timeliness, completeness, and accuracy. In all cases, the importing organization must be able to successfully generate all required reports but not limited to the APR and the Michigan Basic Counting report.
    b. Agencies exporting data from MSHMIS must certify the privacy and security rights promised to participants on the HMIS are met on the destination system. If the destination system operates under less restrictive rules, the client must be fully informed and approve the transfer during the intake process. The agency must have the ability to restrict transfers to those clients and approve the exchange.
2) MSHDA/MCAH and/or the CoC may elected to participate in de-identified research data sets to support research and planning:
    a. De-identification will involve the masking or remove all of the identifying or potential identifying information such as the name, unique client ID, social security number, DOB, address, agency name and agency location.
    b. Geographic analysis will be restricted to prevent any data pools that are small enough to inadvertently identify a client by other characteristics or combination of characteristics.
    c. Projects used to match and/or remove identifying information will not allow a re-identification process to otherwise de-identified data sets. The organization/person changed with retaining that data set will certify that they meet medical/behavioral health security standards and that all identifiers are kept strictly confidential and separate from the de-identified data set.
    d. The CoC will be provided with a description of each study being implemented. Agencies may opt out of the study through a written notice to the CoC or the study owner.
3) MSHDA/MCAH and/or the CoC may elected to participate in identified research data sets to support research and planning:
    a. All identified research must be governed through an Institutional Research Board including requirements for client informed consent.
    b. The CoC will be provided a description of each study being implemented. Agencies may opt out of the study through a written notice to the CoC or study owner.