Michigan Statewide Homeless Management Information System

Privacy and Confidentiality

SP 5.x

6-15-2011R

Session Logistics

- Handouts:
  - Training PowerPoint
  - User Agreement/Code of Ethics
  - Privacy Completion Test
  - Privacy Training Packet
  - List of Basic Agency Requirements
  - Sample Privacy Script Language
  - Privacy Workflow Examples

Session Logistics (2)

- To receive your Trainer of Trainer Privacy Certification:
  - Attend a Privacy Training with a Certified Trainer.
  - Take the Privacy Completion Test
  - Fax or email Completion Test to Gloria Percora:
    - MCAH, PO Box 13037, Lansing MI, 48901, gpecora@mihomeless.org, Fax: 517-485-6682
  - After we receive and grade your test we will email you a certificate. Be sure your contact information is legible!!

About MSHMIS

- Congress directed HUD to “Collect an array of data on homelessness in order to prevent duplicate counting of homeless persons, and to analyze their patterns of use of assistance, including how they enter and exit the homeless assistance system and the effectiveness of the systems.”
- Improve services to clients through coordination of care and better access to resource information.
- Web based - aggregates common information at the agency, community and state levels.
- MSHMIS is administered by the Michigan Coalition Against Homelessness (MCAH), contracted through MSHDA (Michigan State Housing Development Authority).

The Operational Privacy Rule

- Decisions about sharing records through MSHMIS are made by the participating agency with informed client consent.
  - Agencies decide what other agencies they would like to share with to create a single point of entry and/or to coordinate care.
  - Agencies decide what parts of the client record is shared with whom. Different parts of the record may be shared with different partners.
  - The client agrees to the sharing with regard to his or her information.

Agency Privacy

- The MSHMIS Participation Agreement limits the publication of agency identified aggregated data. Issues addressed include the fact that only the organization may approve publication of data specific to that organization. However, transparency in review of local performance is encouraged to support local assessment of performance.
- A CoCs are asked to have a reports committee to guide local publication.

The Critical Role of Paper Forms

- Agencies should plan to have paper forms on site.
  - To collect information that is saved for entry later.
  - To insure that staff can use paper if your system is down, if there is a power outage, or if MSHMIS/ServicePoint is off-line.
  - To allow staff to continue to work with clients if a system issue/ question arises outside of business hours.
  - **Questions on Forms should flow in the same order as the questions on the database to ease entry & improve data quality.**
  - Basic paper forms can be found on the MCAH Web site in the Documents Center under Assessments or Funding Requirement.

http://www.mihomeless.org/MCAH/Document_Center/Document_Center.html

Governing Laws, Statues, Administrative Rules

- The MSHMIS Privacy Plan was developed with input from Mental Health, Drug and Alcohol Treatment, HIV/Aids and Domestic Violence to allow those programs with the most restrictive confidentiality guidelines and needs to participate in the HMIS.
- The MSHMIS Privacy Plan has been through extensive legal review beginning with MSHDA, whose legal staff collaborated in document preparation. Agency Lawyers and Executive Directors reviewed the plan during the Pilot process. Finally the Plan has been reviewed and approved by Michigan’s Attorney General.

Domestic Violence Providers

- Domestic Violence Programs are proscribed (forbidden) to participate on the HMIS.
- The Law does <u>not</u> apply to DV survivors that seek services from none-DV providers.
- Domestic Violence agencies may assess risk and provide their clients – that seek services outside the DV agency - instructions to request that their data be entered as "un-named" and/or that their data not be shared.

Each Provider Agency must adhere to the following:

- All MSHMIS Standards
- Laws, Statutes, Admin. Rules specific to the services provided by the agency (i.e. mental health, substance abuse, etc.)

Review Questions

- MCAH cannot publish your agency identified aggregated numbers without your agency’s permission?
- Who makes the basic decisions about what is shared with whom?
- What is required to share any particular client’s data.

Basic Privacy Rules

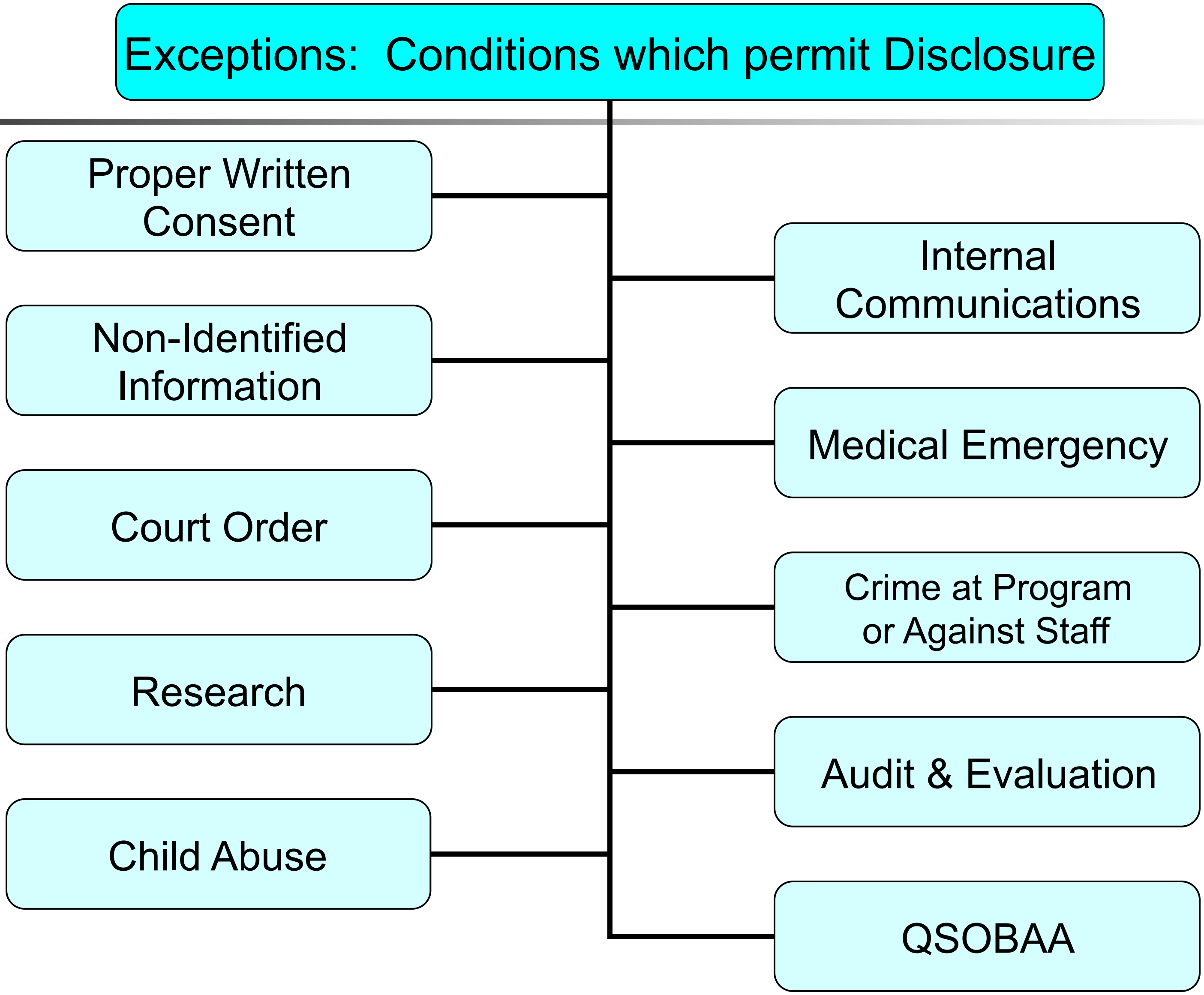
- The Agency’s Privacy Notice is available to all clients. It must be posted on the Agency Website if one exists.
- Agency will not collect or share information unless it is essential to providing services, program management, as part of approved research, or as required by law.
- Agencies will assign each staff an appropriate “Access Level” based on a need to know.
- Agency will not divulge confidential information without informed client consent.

Core Principal

- Clients cannot be denied services that they would otherwise qualify for based on a refusal to share information.
  - One Exception -If sharing is a prior requirement of program participation such as in a true collaboration where staffs work together, the program may continue to operate on that rule.
  - Can a client refuse basic entry? Only if that is your agency policy. However, **there is implied consent for basic entry when information is given at intake**. Many programs require basic records to provide services and report to funding organizations. The system offers an “un-named” entry option if privacy is a special concern.

HIPAA General Rule

Individuals and/or Entities are prohibited from disclosing any patient related information



Exceptions: Conditions which permit Disclosure

Proper Written Consent

Non-Identified Information

Court Order

Research

Child Abuse

Internal Communications

Medical Emergency

Crime at Program or Against Staff

Audit & Evaluation

QSOBAA

Screening for Safety

- All organizations must screen clients for privacy issues.
- Through the Privacy Notice and the Release, MSHMIS makes clients a partner is the core decisions related to data sharing.
- If a risk is identified, agencies are asked to help clients communicate their preferences with other participating agencies.

Privacy Notice

- MCAH provides a sample Privacy Notice for organizations that do not currently have one.
- MCAH provides a "grayed" sample Notice for those with existing Notices indicating what will need to be added in the Notice or an Addendum.
- Remember to put it on your Web Site.
- **All staff must read and understand the Agency's Privacy Notice.!!**

Privacy Notice – The “Script”

- Oral explanation of the Privacy Notice is planned by the agency – a “Script” is adopted reflecting the type of service, the type of information, and any planned sharing.
  - Bullet highlights summarizing key points of your Privacy Notice and your sharing plan.
- The staff provides the Privacy Notice / Script to the client and explains the Notice.
- The Program displays the HUD Public Notice regarding MSHMIS.

The MSHMIS Release/ Acknowledgement

- A MSHMIS Release (if sharing) / Acknowledgement (if not sharing) accompanies the Privacy Notice.
- Because each record can be completely closed, the Release is designed to obtain client consent regarding the use of the “Client Profile” search screen and data sharing - NOT basic entry.
- When closed, MSHMIS operates like any other internal record-keeping system. The Release is simply an acknowledgement of the Privacy Notice.

Developing Your MSHMIS Release

- See Typical Sharing Configurations Draft Releases (mihomeless.org)
- The version of the Release selected reflects the agency's decisions regarding sharing and the "Client Profile."
- If interagency sharing is planned an attachment is developed identifying what is shared with whom. The attachment reflects the agency's signed Coordinated Sharing Agreement(s) – Sharing QSOBAA.

About the Client Profile Search Screen

- The Profile is the only open default on the MSHMIS. It includes the name, the Year of Birth, the Gender, and the last 4 digits of the SS# with client approval.
- The Profile is used from the "Search Screen" to select client record, to enable the sharing of records, and to reduce duplication in the system – a client gets one, and only one, identifier.
- The Client Profile does not disclose where services are being delivered or what services they are receiving.
- The Profile may be closed as needed. This will prevent all but the serving agency and any planned sharing partners from seeing the name on the search screen.

MSHMIS Release Step 1: The Profile – Client Search Screen Determine how identifying information will be handled.

- The Profile should close if:
  - a. The client is concerned about someone knowing they have sought services even if no information about the specific service is given.
  - b. The client has friends, family or enemies who work in MSHMIS participating agencies.
- The Profile may be closed by clicking the "security" button. The Profile may be closed to all or restricted to a small number of exceptions/sharing partners.
- When removing external sharing be sure to leave programs within your agency unless otherwise specified by law.

Determining if addition protections beyond "closing" the Profile are need – Using Other Entry Options:

If the client is at <u>significant</u> risk, is well known, or has a relationship with the agency itself (e.g. the child of a Board member), closing the Profile may not be enough.

- The "Un-named" record:
  - If risk is identified for the client, MSHMIS offers an interface that does not include the client's name or SS#. Further, when a client is entered using this interface, they may <u>not</u> be searched using any identifying information – the name and SS# do not exist on the System. This interface does however allows for unduplication to occur. Use of this interface is connected to User License permissions. Agencies may adopt an "un-named" interface for all entry, or may use if just for clients with additional risk.
- Because we offer Un-named records and clients sometimes change their names, **be sure to write down the Client Number or print the opening screen** and keep that secure. If you lose that number, you will be unable to find the record in the future.

MSHMIS Release – The Profile Cont.

- If the client requests a closed profile and you find his/her name already on the open Client Profile pick list, complete the following steps:
  - Do not click on the open profile that already exist. Call the MCAH Help Desk and we will help you take steps to close the profile retrospectively.
  - An explanation of coordinating the closing of a profile is included on the MSHMIS Release.

Final issues related to Profile

- Because we allow users to close of the Profile, it is very important that you **carefully enter the first and last names, DOB, and gender**. These fields are used by the system to identify duplicate records. They are the most important fields in the System.

- In collecting the name, DOB, and gender we ask that agency staff request and ID if at all possible. Names should be entered as they are on the ID.

- Staff are the first round of de-duplication. You know your client! Be sure to always use the record associated with that client. Ask the client if they are in the System under another name. They should know. You may update the name as appropriate.

- Use only the last 4 digits of the SS# to support identification.

MSHMIS Release Step 2: Sharing

- Does the Client agree to the Sharing Plan defined in the agency's Sharing Agreement(s)/ QSOBAA? The Client approves the total Sharing Plan or does not agree to share .
  - All screens included in the sharing plan have the same basic risk.
  - All questions within the screens have the same basic risk.
  - The client is provided information about what is shared with whom.
  - If the client does not approve the sharing plan, **staff should tailor visability to exclude external sharing. Remember the electronic ROI is required for both internal (does not require a signed Release) and external (does require a signed Release). When you share externally with a specified end date, you must enter a new ROI to continue internal sharing after the old one expires.**

MSHMIS Release Step 4: Signature/End Date

- An end date is negotiated for the MSHMIS Release. To optimize the coordinated care and to reduce the complexity of managing the ROI, the client is encouraged to **select a date that spans the length of time the client is likely to participate in the program.**
- If new information is entered after the expiration of the ROI, the information will not be shared. **You must obtain a new Release prior to entering new information if that information is to be shared. The default rules applied at data entry continues for the life of the data.**
- Without an ROI or when the staff closes a record, MSHMIS operates like any other internal automated record-keeping or reporting system. The sharing functionality is disabled.

Release Confidential Information

Finally, the Client is informed that if confidential information is included in the information collected, he/she will be asked to approve a second release to allow that information to be shared.

- Progress or psychotherapy notes;
- Diagnosis, treatment, or referrals related to a mental health disorder, drug or alcohol disorder, HIV or AIDS, and domestic violence concerns.

- This information shall NOT be shared with other participating agencies without the client’s written, informed consent.
- Sharing of confidential information is NOT covered under the general MSHMIS Client Release of Information.
- The Release is signed and logged onto the System prior to entering confidential information.

Release Confidential Information

(continued)

- What do you do if a benign field reveals restricted information? For example, a client indicates a treatment facility in the current residence field?
  - Complete the second release for restricted information with the client.
  - Staff should close the impacted screen by clicking on the “lock,” if the client does not want the data to be shared or if staff wishes to simply close the assessment.

Review Questions

- A client can be denied services that they would otherwise qualify for because they refuse to share information with another agency?
- Agencies must provide clients with a Privacy Notice/Script, the MSHMIS Release / Acknowledgement, and a second release if sharing includes confidential information.
- What information is viewable for all approved users from the Search Screen - Client Profile?

Review Questions

- The Client Profile does not disclose where services are being delivered or what services a client may be receiving.
- What are the four most important data elements to enter correctly into the System?
- You are required to disclose the full SS#.

Sharing Rules in SP 5.x

- The basic rules for sharing data through the HMIS have not changed. That is, the agency decides what is shared with whom and the client provides "informed consent" to that sharing.

- Rather than setting "sharing exceptions" to the closed environment, in SP5, agencies establish sharing via "visibility" and/or Visibility Groups.

- Sharing is a "planned and purposeful" activity that is governed by established policy and procedures.

Two Basic Advantages to Sharing in SP 5.x

- Sharing set up is much easier. Visibility can be created for an agency and all its children by simply pulling the agency. If the agency adds provider pages the visibility automatically adjusts.

- Through visibility groups, SP 5.x also offers the ability to share retrospectively within an agency if they add a program.

- More detail on Provider Groups and sharing through 5.x is provided at our Web Site 5.0. Training is also available live or in our Podcast www.mihomeless.org .

Rules of the Road for SP 5.x Sharing

- Retrospective sharing is not allowed for "external" sharing to other agencies without informed consent from the client.
- If an Interagency Sharing QSOBAA has been established and a new agency wishes to join that QSOBAA, the "external" Visibility Group that allows sharing must be closed and end dated and a new Visibility Group established to which the additional provider (s) are added.
- <u>Any modification of external Visibility Groups (once established) will result in a violation of privacy unless all clients impacted have agreed to the retrospective sharing</u>!!!
- **<u>Never delete a Visibility Group as all sharing covered under that Group will terminate.</u>**

Computer Security

- All computers that directly connect to the internet must have a properly configured firewall, current anti-virus and spyware protection, and the most current patches, upgrades, or hot fixes.

- All servers must be protected by a firewall, current anti-virus, and current patches, upgrades or hot fixes.

- All computers used to access MSHMIS must be secured from public use.

- Required Internet Tools settings:
  - History to 2 days, and
  - **Delete temporary files on exit.**

- 5.0 requires a large temporary file cache for a single session. To support use of 5.0, please adjust your cache size when you complete the above settings.

MSHMIS Security

- All transmissions over the internet are provided industry-leading 128 bit AES encryption.

- Client information is stored on a server in a locked bank with controlled access in Shreveport, LA.

- The application is on a server separated by a second fire wall from the server that contains the data.

- Multiple security tests have been conducted including professional “hackers” to assess data security.

Agency Responsibilities

- MSHMIS is a prioritized process within the Agency.
- System users complete formal training on Privacy and Confidentiality provided by certified trainers.
- Agency leadership ensures that system users abide by the privacy rules.

Agency Responsibilities Cont.

- Agency leadership adapts the MSHMIS Release and the Privacy Notice to reflect their sharing decisions and in compliance with core standards.
- The Agency has a Board Certified Confidentiality Policy. With regard to the HMIS, the Policy must reflect the privacy rules that you have learned today.   An example policy is provided by MSHMIS.

Required Meetings

- Local System Administrators (SAI) are required to attend the monthly SA Call-In.
- Information from the Call-In and local use issues are address at routine CoC Agency Administrator Meetings. The frequency of those meetings will depend on the size of the community and issues currently being addressed.
- Agencies are required to routinely review their data quality and address internal issues.
- Agencies receiving funding and reporting through the database are required to routinely attend training and meetings.

Review Questions

- SAIs may not add new agencies to an existing External Visibility Group.

- MSHMIS provides the highest level of transmission encryption possible.

- What Meetings are required to participate in the project?

Privacy is a culture:
Common Violations – About Releases

- Staff having clients sign “blank releases” in order to fill in at a later date when staff need them.

- The use of “General Releases” (prohibited by state and federal law).

Common Violations – Culture

- Staff disclosing client information to 3rd parties without client authorization.
- Staff discussion within professional settings - “informal case discussions” that occur on-site where other’s without a “need to know” may overhear.
- Staff discussion outside professional settings – case discussions over coffee in restaurants.

Common Violations - Culture

- Staff identifying individuals as clients at social events and/or self help groups.

- Agencies and staff failing to establish and/or inform clients of the rules related to privacy and confidentiality when participating in group sessions.

- Staff identifying clients (without consent) when taking phone calls.

Common Violations - Culture

- Cars --- Where clients park reveals their life choices. This issue can extend to staff who have identified risk as well. Consider personnel policies as well as client policies.
- Client files left in an open area for others to see. Are files in use put away when others are about?
- Unlocked and/or unattended client charts. Is the records room supervised or locked at all times?

Common Violations – Work Space

- Unattended computer screens with client information visible or accessible.
  - Use a screen saver.
  - Close down when you take breaks.

- Attended computer screens visible to unauthorized personnel while entering data (work space configuration).

Common Violations – No 1 Issue Pass Word Control

- Unauthorized use of computer passwords and/or log-in codes
- Writing down, losing and/or sharing your User ID and Password.
- Weak or easily guessed passwords
  - 80% of all security issues stem from poor passwords
    - Passwords are like underwear
      - Change yours often
      - Don’t use other’s
      - Don’t share, even with friends
      - Keep them discreet
      - Don’t leave them lying around

Common Violations -Pass word Control

- Tips for creating strong passwords
  - Use Favorite Phrases
  - Stay away from dictionary and personal meaning words
    - Baseball, charlevoix, family names (bob, sally, etc)
  - Stay away from meaningful dates and number
    - I.e. birthdays, anniversaries, Social Security Number, etc.
  - Don’t use sequences like “abcdefg”, “123qweasd”, “54321”, etc
  - Don’t use reversed words
    - October vs. rebotco
  - Never spell anything correctly
    - October2005 vs 0ktbr25
  - Use upper and lower case characters, numbers and special symbols

Common Violations –Downloads

- Downloads client data on home computers **(No 2 most likely vulnerability).**
  - If completing work at home/approved remote locations, plan for the process, control/restrict downloads, and insure hard drives are properly cleaned.
  - Do not allow data to be transported on “A” disks or other mobile devises without clear guidelines for disposing of those devises.

- Identify and secure computers within your agency where client information exists.
  - Agency failing to have proper security for storing, retrieving, and accessing client information. Any file (word, excel, etc) with client identifiers on an agency computer should be secured.
  - When “swapping out a computer” be aware of what is on the computer and plan for the cleaning of that hard drive.

About the tools we use.

E-mail and cell phones are not secure.

- Any client related information should be zipped prior to sending via email.

- Staff and clients should be thoughtful about what they say over a cell phone.

Other Issues

- Social Engineering- falling for phone calls or emails in which someone portrays themselves as a trusted resource in order to gain sensitive information
  - Always question who is on the other end of the phone.
  - Never open any emails from those whom you do not recognize, if unsure, call the person that sent the email for confirmation
  - Always ask for a call-back number.
  - If suspicious, say you will call them back.
  - Beware the computer repair person that shows up unannounced

Remember:

You have a professional Responsibility to maintain the individuals “Right to Privacy”

There are penalties for violating the client’ s “Right to Privacy”

Tracking Privacy

The System provides a tracking of all individuals who have "touched" a record within the system, assuring personal accountability regarding what is done within the System.

Minimum Data Entry

- Organizations that have very brief contact and do not complete a detailed intake interview should enter at minimum the **Universal Data Elements**.
- For agencies that conduct an detailed interviews, HUD requires/recommends that at minimum organizations complete the **Michigan Statewide Entry/ Exit or a Funding Specified Assessment**.
- CoC's may also develop a local question set that includes questions of local interest and/or those not included on the Michigan SW but of local interest.
- A suite of Outcomes is provided through the HMIS and largely rely on the Universal data elements. The Self Sufficiency Matrix and/or Case Plans are available for more individualized goals.
- Other Assessments may be selected by your Agency Administrator.

Data Quality

- Each User will have a a very structured workflow - the steps to complete data entry. Workflows should be specific to job function and should be rigidly followed.
- Paper forms that model approved workflows are available on www.mihomeless.org.
- Agencies are required to monitor their data quality.
- ***All programs should run reports monthly to assure that data entry is accurate, timely and that your workflow is appropriate.***
  - When you begin data entry check to make sure that the reports are appropriately reflecting the data that you entered.
  - Agency Leadership must review the Reports to insure that staff are correctly applying the definitions. Of special interest is the HUD definition and how you enter prior living situation/ where the client was on the night before admission.

To Go Live:

- Agencies must sign an **Administrative QSOBAA** (Qualified Service Organization Business Associates Agreement) that will assure that all organizations (local lead agency, MCAH & MSHDA) involved in the administration of the System may not re-release record level/ identified data. That agreement also requires that the Lead Organization resist subpoenas in the same manner that a service organization would, and to maintain the data in a secure manner, meeting all confidentiality requirements.

- Agencies must also sign a **Participation Agreement** which reflects what you have learned today. That agreement is between MCAH and the participating agency.

- All Users must carefully review and sign the **MSHMIS Users Agreement**. That agreement must be kept on file.

MCAH Web Site

- The MCAH Web Site contains:
  - A List of Organizations that can see the Profile statewide is provided on the MCAH Web Site.
  - The most current version of all the Forms and Documents.

www.mihomeless.org

Final Review Questions

- What are the two most common privacy risks associated with all automated records?
- It is critical to run reports frequently.
- What 3 documents are required to Go Live?

SEND IN YOUR COMPLETED TEST