Overview of Privacy Recommendations
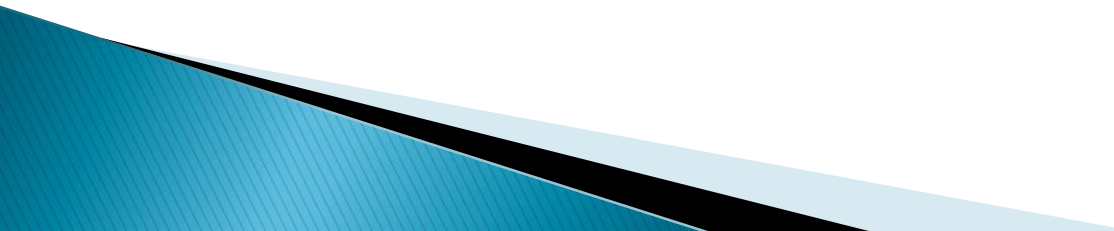
I. Review MCAH Privacy Recommendations

II. Review Sample Privacy Statement that summarizes our values.

III. Review of the Privacy Concept Decision Chart that includes:

    I. Issues

    II. Michigan Model

    III. Current Practice

IV. Discussion

V. Governance votes on Issues

Establishing Trust

▸ A <u>clear, coherent, smart privacy rule</u> is required. Our Privacy Protocol was carefully developed, has stood the test of time, and allowed diverse participation.

▸ Michigan operates with one of the most <u>conservative</u> rules in the nation and yet has more actual <u>data sharing</u> than almost anywhere in the nation. It is a Gold Standard Product.

▸ <u>Reduces conflict</u> at the local level and <u>improves risk management</u> for SA/LSAs.

▸ A privacy rule that <u>allows everyone that needs to participate participate</u> including: mental health agencies (Path, S+C, HOPWA), drug treatment programs, community health, education, and Runaway and Homeless Youth. These programs have been engaged for years. <u>You can lay almost any privacy rule over the top of our operating procedures. PRIVACY IS NOT A BARRIER!</u>

▸ **It respects the professionalism of the agencies and recognizes their protective role in the lives of the clients they serve.**

The Michigan Basic Privacy Rule:

- The Agency decides who they would like to share with and what needs to be shared. They can and do share different things with different agencies.

- The Consumer decides whether or not their particular information will be shared via a very structured Informed Consent process.

- Sharing should always benefit the consumer.

- Sharing should be an affirmative act – no default sharing beyond the Search Screen and that may be closed for cause.

- Providers that share information with one another must talk to one another to use the data & negotiate conflicts.

- Sharing is a privilege not a right. Data quality and data security processes must meet basic standards.

What is sharing?

- **What is Sharing:** Sharing involves the exchange of data between agencies for the purpose of coordination of care.
  - Sharing a Case Plan between agencies to coordinated set of objectives.
  - Coordinating between shelters and service programs for high risk consumers.
  - Coordinating Street Outreach interviews with recommended service providers.

- **What Sharing is Not:** Data entry into the System. Most service systems (hospitals, behavioral health programs, your dentist) are required to keep a record and today most records are electronic. Records are necessary to support continuity of care and accountability to funding sources as well as internal Quality Programs. There is **"implied consent"** for keeping such a record when services are requested.

- **Risk Management:** If a consumer or agency has identified specific risks (and we teach what those risks might be), we offer a variety of strategies for reducing exposure from closing the record to entering it as "un-named". Privacy begins with knowing your customer.

Privacy Evaluation Finding: Currently NC requires agencies to ask if the client wishes to "Opt Out" – a choice that significantly impacts and limits the basic utility of the System.

- Impossible to count or project numbers because you can't unduplicate. Statewide or CoC numbers would require an off-line matching and unduplication. This process will result in higher risks for all clients as it would require multiple off-line record sets with PPI that then have to be controlled.

- The basic funding reports (APR, ESG, etc) cannot be done as one-button reports and because they are produced off-line and the analytics are so complex they are very likely wrong. We hear that it is very hard and ungratifying work to generate reports and at least part of that stress relates to this issue.

- The informed consent process itself is unstable. The %/# of "opt out" varies from one agency to the next (some agencies had quite a few and some almost no one) and there does not appear to be specific controls necessary to make this consent process "informed". Opt Outs very likely reflect the privacy bias of the specific case manager/agency.

- If you legitimately ask the question, some clients will say "no". All agencies must be ready to maintain additional record systems.
  - Do you then ask the question as to whether it is ok to keep a record in these alternative record systems. Have to explained the risks associated with those Systems.
  - There is no evidence that those alternative Systems are safer. Record systems processes within agencies that do not benefit from certified records specialists would not be safer.
  - What does the agency do about other funding sources such as SSVF or RHYMIS or other state and local funders that require a record reported to a funder? Line staff would have to know which clients to ask and which to not ask. Mistakes will be made.

Discussion Privacy:

- We want you to adopt our Rule: Some discussion points:
  - Reduce search screen information to name, year of birth, gender and last 4 of the SS#

  - Make "Consent for Data Entry" optional to the agencies. Basic processes are controlled at the agency level so if an agency does not agree they are likely to leave the system or do a poor process of making the ask.

  - Remove global defaults that exist in your current System. Some parts of the system are wide open for anyone to look at. This is not purposeful sharing. I as a consumer cannot simply ask where my data has gone.

  - Turn on <u>or</u> off the "Release of Information" functionality.   If we turn off the Release of Information it will reduce many typical problems with sharing, however it means that processes for closing the record when the client says "no" have to be very stable. Potential breaches of data are more likely.
    - The ROI merely reflects the response on the Release and does not impact actual sharing. Sharing is solely controlled on the Client Record either by closing the Profile or closing specific Assessments.

  - How to roll out the Training (how much Live/Live GTM/Recording)

  - What do we do about the Database Encryption that currently exists.