**Data Evaluation Committee Meeting Notes**

Wednesday, December 16th, 2020

8:30– 10:00am

Present: Regina, Owen, Jonathon, Cynthia, Michele, Noemi, Shaundell

**Data Goals:**

There is some work ongoing in other parts of the CoC that is related to data and some new goals have been identified that this committee might be involved in. The Youth Homelessness Demonstration Program has a consolidated community plan which outlined some goals both for projects and the system as a whole. This committee might look at some of the results of that project level data and performance results and might try and help the CoC determine if they are meeting identification goals. If there are youth which are in need in the region and not connecting with the CoC for some reason, the goal is to identify who those youth are and what barriers keep them from accessing services in order to make CoC services more accessible and ensure we are supporting all youth.

There has also been work done by the Racial Equity Workgroup to create a racial equity plan which has a dedicated data goal. This goal includes a few action items including conducting specific racial disparities analyses on coordinated entry data, identifying high acuity disparities every year to tackle specific problems, and working on cross-system data sharing. All of these action items will likely involve other committees (such as the coordinated entry committee) or partners but the Data Evaluation committee will play a part in supporting these goals.

Trauma informed data collection training – As part of the YHDP process the CoC is going to hold two trauma informed data collection trainings in January. The first will be a general overview with some roleplaying of more difficult scenarios and questions and the second training will focus on some data that the CoC asks only of youth and can be especially sensitive such as sex and labor trafficking and sexual orientation and family substance use.

Michele will provide everyone with more updates/information as soon as we know more but has confirmed that we will invite the data evaluation committee to participate when we send out the training details in addition to partner agency staff.

Jon- when we were looking at our data it looked like some of these numbers seem small, some demographic groups weren’t well represented, how do we account for that?

Noemi- This might be reflective of people feeling hesitant to engage with the system

Owen- there are some ways to account for this, like with size, or separate out to look at trends across the groups. Dial/Self tries to look at the same group of people from different angles.

Noemi- It's worth thinking about how people from different communities tend to manage their homelessness. Young trans people who are white manage homelessness different from teen parents and latinx people. Some real questions about who is being recruited and accepted and is within the context of these data goals. Also, worth thinking about what we know about people who couchsurf and don’t access services. Why are people not showing up for services if we know they exist in this community? Particularly young communities compensate for what they perceive to be families.

Cynthia- I could see the point in time count could be improved but what can we know about this CoCs limits in terms of the population that we’re getting data on? Getting data on people who are chronically homeless, how does this come into play? In general, we’re getting detailed data on people including demographics.

If data collection is expanded for youth, then shouldn’t we expect to see more diversity?

The racial equity group is helping by identifying ways to prioritize people from a wider range of situations, the data could become more diverse.

**Privacy and Security Plan**

We spent the remainder of the meeting continuing to review the Privacy and Security Plan from the previous meeting:

Jon- The Compliance Certification checklist is very important to keep computers secure and data protected but understand that agencies might not have ability to do so often if they don’t have much staff.

Cynthia- if they have support from Michele and know what they need to do, don’t think it will be too burdensome, feel the same as Jon, this needs to be done regularly to keep things up to date. Having support is very important- Kathy emphasized knowing ahead of time what this process would entail.

Agency Security audits – right now the plan says that each agency security officer will compare employee login times with time sheets and there is a concern this is too much.

Owen- is the intention that going in to HMIS after hours is nefarious? No one really wants to be doing after hours data entry.

Jonathon- if employees are logging in when they’re not supposed to be on the clock, we should look into why. If they don’t have a really good reason for being in there, we should look into that. These protections serve an important purpose.

Cynthia- maybe this is something the new HMIS system can work with?

Jon- can the system flag this? In the HMIS? If employee work times are entered?

Noemi- noticing something, this is an attempt to catch anomalous access at the core. Maybe the problem can be addressed without meaning timesheet audits?

Right now the language helps the partner agency security officer- if there was a process in place for determining this was a legitimate access of data.

Owen- Great point, this is very applicable to work at Dial/Self. Used to be a case manager and have trouble getting people to log in frequently enough to do data, feel like on paper something like this looks useful, instead it seems like someone will have to spend a long amount of time getting everyone’s schedules and log ins. Now staff feel put under a microscope. Understand that security is extremely important but feel the merit is outweighed by the burden of doing this and creating an environment where staff are being watched.

Michele- can we implement 2 factor authentication?

Owen- like this idea, might be difficult for some staff to learn but ultimately could be helpful as they could implement 2-factor in other places as well.

Cynthia- still want to keep in idea to certify not using remote access/own computers. Might want to ensure that staff have access to agency computers.

It is not something we included in our RFP but will inquire with the vendors who submitted HMIS proposals if they can incorporate 2 factor authentication.

The current plan also asks partner agencies to notify the CoC within 15 days which the group felt was too long if there are serious problems.

Cynthia- checklist could have different levels of action items- within 15 days is the outside and there may be some things that we say to notify us immediately.

CoC Security Audits- right now the plan states that the CoC will randomly audit 10% of an agency’s workstations annually.

Owen- this seems adversarial to have Michele going to agencies and doing random audits. Seems like a waste of time, seems like it could cause ill will

Cynthia- this is an audit feature that goes along with other kinds of audits at program level. Fiscal, record keeping, etc.

Jon- It shouldn't be considered adversarial to have checks and balances and make sure everything is going well.

Noemi- is there a happy medium, instead of directly auditing workstations, can partner agencies be expected to produce a log of these things and we audit the logs?

Owen- I love that, currently have some form of log and could create an inter-agency log to check things. Could be a tier above if there is a suspicion that something is going on. 10% or 30 would take Michele several workdays per agency and then what is he not able to do while doing those audits. Absolutely agree that having checks and balances is an inherently valuable component and that really matters the most for making sure agencies are working with youth and populations they are being paid to support, money is going where it should. Cybersecurity component is extremely important but this level feels beyond reasonable expectation and burden.

Jon- would be a good in-between if agencies reported list of things to the CoC, then they would still have that check in place.

Owen- there has been a lot of work to ensure my position exists which doesn’t at many other agencies. Probably are other agencies that aren’t doing this now, how can we support them without taking up inordinate amounts of time?

When would these audits happen? Are they just without their computer for the middle of the day?

Jon- would there be a way to wrap it into the compliance certification checklist? If there is a security breach then it would fall on the agencies shoulders since they are certifying everything is good.

There is some more discussion to happen around the CoC-level audits but the group seems to feel that asking partner agencies to submit a log of their audits as part of the checklist may be a good alternative. Michele will double check that this isn’t a HUD requirement.

Physical safeguards:

The first physical safeguard is that computer locations must be in secure locations where only authorized people (those who have gone through HMIS privacy and security training in the past 12 months) can access them.

Noemi- is this actually happening now?

Jon- in new york the secure information was in a separate room always.

Owen- lots of people have laptops, if they are password protected and encrypted, this would likely meet the requirement, right?

Not sure if computers are all in a locked space now, Michele will check if this is another HUD requirement or recommendation and what would complete this requirement for mobile devices.

Noemi- An appropriate data practice is to not hide the screen from clients. Strong advocate that people should have the authority to report/represent how they want to.

Michele mentioned that HUD encourages CoCs to enter data they know is accurate if it will help a client receive services even if it differs from that person’s response or beliefs about themself, which could make it difficult to view screens with clients

Noemi- This shouldn’t be the case- I believe in following client choice and how they want to represent themselves or be reported to a federal agency.

Owen- Meeting people where they are at is important, we would probably want to talk with people and meet them where they’re at. Never did data entry in front of youth. Would look at bus schedule or craigslist for jobs with youth on computer- lots of viable reasons for sharing work screen, not just doing work for them and not doing it by themselves, but together.

Consider common sense, close the data system when sharing the screen but there are lots of reasons why we might want to share a screen with clients.

Noemi- Flip side to the hypothetical situation is important- if a case manager is entering data to help people get services it’s good to explain this to participants. People are often so lost in state and federal benefits that down to earth leveling about how to access is vital.

Michele- lots of staff are doing paper intake and then doing the data entry later in normal circumstances.

**Closing & Next Meeting**

Our next regular meeting would be March 5th, 2021 and there is a concern that this is too far away as we have not finished our work on the Privacy & Security Plan and need to tackle the Data Quality Plan as well. We agreed to determine our next meeting by Doodle poll but Michele is suggesting we meet at our regular time on the first Friday of February instead. If this does not work we will determine our next meeting date with a doodle poll.