Data Evaluation Committee Notes

6.23.21

Present: Owen, Shaundell, Justin, Brooke, Michele, Kathy, Matt, Paige

**Where are we now?**

Discussed the current status of our work and the HMIS implementation, we have a barebones system setup and are currently gathering agency and program configuration information in order to build out projects in the new HMIS. Once that is ready we will begin the data migration process. There is a tentative ‘Go Live date of December 7th and we would like to be prepared with our agency and user agreements before then. This committee will be doing a lot of the work around these agreements by determining our Privacy and Security Plan and Data Quality Plans, both of which will inform our participation agreements.

**Are there volunteers for a co-chair?**

Kathy- how about Owen?

Owen- thought about it, not sure has the ability to commit to it but will let us know if that ever changes. Happy to see so many people in this meeting so we can make some inclusive decisions around policies that will affect everyone in the CoC

There’s time for everyone to consider if they would like to act as co-chair, please reach out to Michele at mlafleur@communityaction.us if you are interested.

**New HMIS Implementation Updates-** Go Live December 7th

1. **Need to have agency and user agreements ready for going live**

 **B. Very configurable, need to make multiple decisions: 2-Factor Authentication, requiring release of information (ROI) on client creation, sharing data across agencies, user policy enforcement? If sharing data, how much? Would this require a change in our ROI? Would it require MOUs or agency sharing agreements?**

Matt- having a required release of information sounds like a good idea, especially as we’re moving towards data sharing as it sounds like we are. Would be good if that can be so that people can specify who their information is shared with in the release and then have that be reflected in the HMIS.

Matt- Most releases are 6 months to a year but if we change it, we need to go back to resigning. Put in a note about who can see data in the release and state that at some point we may open up to share. With access we may run into some technology issues. Turning on and off access to other agencies

Paige- in regards to two-factor authentication, encounter a lot of people who don’t have cell phones or don’t have that technology and it could be a barrier for some people

Owen- two factor authentication, just for staff, right? (Yes!) Love the idea of rolling out 2 factor authentication. but want to make sure agencies are equipped to use it

Kathy- a little concerned about Louison House troubleshooting this

Owen- yes, it would be a burden but that may be outweighed by the security benefits? Definitely hesitant to add barriers to staff doing data entry

Justin- Are we pushing this to be mandatory or is it optional? It might be helpful for some people but could be tough for others. Maybe if it’s something that you want personally it can be turned on, but it doesn’t have to be mandatory.

Owen- could get tricky if you don’t have access to the device you use for 2 factor on hand and then lose access altogether. We’re trying to improve security but now someone can’t get in to the data system and maybe needs to create a new account and open up other issues.

Michele- What about an option to decide agency by agency or user by user, might be a better option than required for everyone?

Justin- agree that it could be prohibitive and not be the best option for us to require everyone to use 2-factor

There’s also an option to force password changes every 30-360 days, can determine exactly how many days later.

Owen- password changes too often probably isn’t going to help a lot, probably a middle ground in frequency of changing passwords. 90 days or 120 days, a few times a year but not continually changing. Already going to be moving from one system to another, the more things we change the more difficult it might be for end users

Justin- don't remember ever having my password changed, using ETO for years. If there’s a decision between one or the other I would rather it force us to create a set password over 2 factor authentication

Owen- it's more accessible to change passwords regularly than employing and maintaining 2 factor. Important we don’t assume staff know the same things we know, many people may have to learn 2-factor. Thinking through assumptions we can make.

**Optional two factor authentication with required password changes every 90-180 days seems to be the way to go, we can determine the exact time frame for password changes another day.**

Looking at sharing option next: Not shared, basic shared, or full shared. Basic shared lets you see most data but not make changes to data entered by other agencies or see detail of notes, etc.

Michele- full shared sounds like too much since it allows for editing and deleting assessments and forms

Kathy- It could be helpful to use full shared sometimes, especially for CE referrals

Matt- transferring a client from Berkshire to Franklin county, would that require switching or a lot of work? Client we’re housing and have made a referral to MHA, would want to be able to edit their file or close it.

Michele- don't think it would require too much work since it would be a referral from one program to the other and should still be able to work on client file until dismissed (maybe longer? There’s still a lot we have to learn about the nuances of our new system in practice), it’s not really possible to set sharing permissions by client/participant and they are restricted to the agency level.

Kathy- Sounds like a full transfer, but could at times be helpful to have full sharing anyways

Michele-There's also an option to set exceptions for specific agencies, create groups of agencies which share among one another but not outside of that group, etc.

Justin- where does this start? What if the participant doesn’t want information shared? According to the release it seems like it is already being agreed to. Can certain notes or items be hidden until you get comfortable and form a relationship?

Michele- don't think this can be determined by participant but is set by agency. Michele will double check setting things as “sensitive”, which could be an option to hide information in a client file so other agencies can’t see even if there is sharing between agencies

Owen- reading over the release, we’re going to need to change it anyways when we move to a new system. If we were going to talk about a greater degree of cross agency sharing, we could add something to make sure we’re adhering to that. With any degree of sharing comes a lot of responsibility of all staff involved. Instinct is to err on less sharing side but the nature of coordinated entry does intertwine all of these agencies. In an ideal scenario, all agencies working with that person and having access would improve quality of care but getting to that point wouldn’t be necessarily easy.

Michele- think this might be dependent on data sharing agreements with agencies within one another, will check in with HMIS TA, but it’s unlikely we’ll be able to make the final decision here, more likely a recommendation to bring to agency/program leadership.

Owen- Yes, should probably leave that up to individual agencies because there are so many different funding sources with different requirements, impossible to craft a policy here that meets the requirements of all funders. Could potentially share agreement with BCRHA to help agencies make policies to support that connection.

**Agreed it might be good to work on bringing this issue to partner agencies and asking if they are comfortable sharing their data and if so, at what level and with all or only specific agencies?**

**Looked at the requirement to include a release of information upon client creation next:**

Owen- In same vein of two factor authentication, the process around uploading documents can be prohibitive. Spend a lot of time getting printers to work properly. Printers are always a challenge, but being able to scan documents and upload them in the system in terms of uploading the release of information is another layer. Is that going to be overly cumbersome if it’s required to enforce a release of information at client creation? At Dial/Self we keep a master spreadsheet of releases and their expiration to see their upcoming expirations, don’t require uploads. Can see this slowing us down or preventing people from entering the data. Some case managers are very busy and this adds extra time.

Michele- looks like it can be built into the system instead of requiring a paper version to be scanned and uploaded, will look more into it and test out in the training site

Owen- if it can be built in that would be a great middle ground, scanning is the biggest barrier, can see it getting overwhelming quickly. How do we make it as easy as possible within reason for staff to do this part of their job? Less complexity is better.

Kathy- concur on all of that, there are staff that aren’t the most tech savvy but are excellent case workers.

Owen- agreed, some of the best case managers are not good with computers

Kathy- enough trouble scanning documents with monitoring, would have to take it somewhere specific for uploading.

Justin- like the idea of requiring electronic or verbal consent instead of uploads.

Michele is going to look into the release of information options in Clarity more closely, it seems that it could be signed electronically or even agreed to verbally, would have to change our release of information but it’s already been pointed out that we have to change it anyways and verbal consent is something we could include, HUD does not care.

**Michele will send out Bitfocus configuration documents with the notes**

**Privacy and Security Plan**

Looking over latest details and the workstation checklist which outlines everything the partner agency security officers will have to check for workstations during the bi-annual security audit. This is a requirement from HUD that we have these officers and audits in place.

Owen- would Windows Defender firewall be appropriate for the firewall requirements? Would be a free, easy option for most agencies. Sounds like a good middle ground and would be acceptable for most people.

Michele- seems like yes but I can double check, Windows Defender may also act as an adequate virus protection but will confirm that as well

Owen- To check every ROI might take a while, maybe it would be better to do a random audit. Is this for all devices?

Michele- Right now our privacy and security plan says that partner agency security officers will conduct security audits on every workstation accessing HMIS every six months but we can revisit this number at next month’s meeting.

Kathy- assume you will do at least a minor training for the security officer?

Michele- Yes, we will work with agencies to get these requirements in place and hold specific privacy and security trainings to explain our new policies. Going forward this will also be incorporated in our regular privacy and security trainings with additional support for agencies as needed.

**Data Quality Plan** – Did not get to during this meeting, but will hopefully look at a very rough draft during our **next meeting on July 28th at 3pm.**