**Data Evaluation Committee Meeting Notes**

Friday, February 5th, 2021

8:30– 10:00am

Present: Owen, Cynthia, Michele, Kathy, Shaundell

**Going over Privacy & Security Document**

In our last meeting there were a few things about our privacy and security plan that were identified as things we needed more information about before we could make a decision. To start this meeting, we began going through these follow up issues.

Do we actually need to have the CoC auditing individual workstations?

FOLLOW UP INFO- The checklist is mandatory but CoC audits of agency workstations don’t seem to be a requirement.

But the HMIS Administrator checklist list this as a duty: “Monitor audit logs for unauthorized access to client records and report deviations from security protocol according to an established channel of communication”

From data standards:

System Monitoring. Baseline Requirement. A CHO must use appropriate methods to monitor security systems. Systems that have access to any HMIS data must maintain a user access log. Many new operating systems and web servers are equipped with access logs and some allow the computer to email the log information to a designated user, usually a system administrator. Logs must be checked routinely. Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by checking user access logs routinely for inappropriate access, hardware and software problems, errors and viruses, or purchasing one of several software applications available that track the status of individual files on computers. These applications are used to make sure that files are not being changed when they are not supposed to be. The applications inform the system administrator if a computer has been hacked, infected with a virus, has been restarted, or if the data files have been tampered with.

Discussion: In general, it seems okay to do audits that are sent to system administrator

And what about using built in auditing tools/programs? This could help take the burden off of everyone

Maybe it could also be built in HMIS?

The Toledo checklist matches what Owen does now at Dial/Self but trying to find a compromise not to burden smaller staff

Cynthia- there may need to be some training to help, IT support can help, the CoC can help

**One in depth annual audit, maybe 2-3 smaller audits seem reasonable. Aim to increase the smaller audits as they get more comfortable and easier for staff.**

Do agencies need to make sure that computers are kept in locked rooms?

FOLLOW UP INFO- Not necessarily literally locked but should be very secure, no matter the chosen method.

From Data standards: Physical Access to Systems With Access to HMIS Data. Baseline Requirement. A CHO must staff computers stationed in public areas that are used to collect and store HMIS data at all times. When workstations are not in use and staff are not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. After a short amount of time, workstations should automatically turn on a password protected screen saver when the workstation is temporarily not in use. Password protected screen savers are a standard feature with most operating systems and the amount of time can be regulated by a CHO. If staff from a CHO will be gone for an extended period of time, staff should log off the data entry system and shut down the computer. Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by automatically logging users off of the HMIS application after a period of inactivity and automatically logging users off of the system after a period of inactivity. Most server operating systems come equipped with the needed software to automatically perform these functions. If staff from a CHO will be gone for an extended period of time, staff should store the computer and data in a locked room.

Cynthia- we should think about reports also, making sure those are kept secure since they can have sensitive information.

Owen- we use Bitlocker, norton antivirus, there are security measures in place but not always a locked door

Kathy- can check with their IT guy but don’t think we should get too detailed because each site needs to figure out something for each- secure is good enough, when staff aren’t present computers are secured from those who shouldn’t access. Be careful with too many details.

Consult with HMIS Lead or IT staff if help is needed.

-Encryption? What about when documents are moved to flash drives, etc.

Owen- email is likely the easiest vector of attack and therefor probably the best place to shore up defenses.

Kathy- don't think the CoC can tell agencies what to do about email, won’t get into 2-factor right now, maybe in a year or two. Advising and telling us possibilities would be helpful though.

Michele- pushing for 2-factor implemented in new HMIS but we won’t implement email policies, although we can offer guidance and best practices/assistance in getting this set up.

**After discussing follow ups front the previous meeting we finished going through the remaining parts of the Privacy & Security Plan**

Removing HMIS access policy:

Owen- this all makes sense

Michele will look up egregious HMIS privacy/security practices as examples of what might result in someone losing access.

Disaster Recovery plan:

Seems largely on the shoulders of the vendor and (right now) DHCD

Cynthia- this could be about CAPVs ability to take action in event of disaster, to communicate with software

After finishing reviewing the plan in it’s entirety and making initial changes, the next step is to solicit more feedback. Michele is going to send our current plan out to our funded project partners and the CoC board for a round of feedback. We will likely need to make revisions afterwards and send the plan for another round of feedback, possibly to other groups as well, such as the Equity & Inclusion Committee.

**Meeting monthly or bi-monthly?**

We discussed whether or not to continue meeting bi-monthly or to move back to monthly as the HMIS procurement workgroup winds down. In addition to the Privacy & Security Plan, we need to create a Data Quality Plan and System Performance Improvement Plan so we would like to meet monthly again if possible.

After discussion scheduling via email after the meeting, it sounds like even though we are planning to meet monthly we are going to hold off on meeting in March to give more time for feedback from partners and to give space for the HMIS procurement workgroup to finish the selection process and enter contract negotiation.