COVID 19 ClientTrack Remote Work Guidance:

As many agencies begin telework practices due to the COVID-19 outbreak, the HMIS team would like to provide guidance from the HMIS Security Plan and Standard Operating Procedures, as approved by the Continuum of Care Board of Directors on 9/19/19.

- Any user accessing the HMIS or DV ClientTrack production systems must be affiliated with an active member agency.
- Unauthorized access is prohibited and is grounds for legal action.
- It is the responsibility of each HMIS and DV ClientTrack participating agency to install virus protection software, with an automatic update on every computer that accesses HMIS, as well as installing an individual and/ or network firewall.
- Agencies must have firewall protection on its networks or computers providing a barrier between the organization and any systems, including the Internet and other computer networks, located outside of the organization accessing the Internet and the application.
    - For example, a workstation that accesses the Internet directly through a modem would need a firewall; however, a workstation that accesses through a central server would not need a firewall as long as the server has a firewall.
- Virus protection must also be in place employing commercially available virus protection software that includes automated scanning of files as they are accessed by Agency Users on the system where the HMIS application is housed.
- Each Agency and IHCDA must also subscribe to virus software, as well as an updates subscription to maintain the virus definitions and code base.
- Whenever possible, agencies should utilize a Virtual Private Network(VPN) to conduct their work during this time.
- Each Agency must establish internal access to data protocols.
    - These policies must govern who has access, for what purpose, and how the information can be transmitted.
    - Other issues that should be addressed include storage, transmission and disposition of this information.
    - Agencies must have written policies and procedures in place regarding the appropriate access to client data in the HMIS and its obligations under the HMIS User Agreement/Code of Ethics.
    - The policies must include, without limitation, when, where and under what circumstances it is deemed appropriate for Agency staff to access HMIS data outside the office.
    - The policies must also indicate the consequences for an individual’s failure to abide by these policies.
    - In addition, the Agency must make every effort through its policies and procedures to ensure that any PPI collected remains confidential, especially at the intake point.
- Any staff, volunteer or other person who has been granted an Agency User ID and password and has committed a breach of security of HMIS and/or Client confidentiality may be subject to sanctions including but not limited to a warning or revocation of HMIS access rights
    - A revoked Agency User may be subject to discipline by the Agency pursuant to the Agency's personnel policies. Agencies must establish and maintain all necessary processes and procedures to properly and immediately close and remove all system and network privileges and resources when an employee is terminated including notifying IHCDA to disable the account.

- The HMIS is redundantly and physically backed up by the HMIS Software Vendor in accordance with all current HUD requirements.
- All Agencies should have a disaster plan that allows uninterrupted business access to the Internet for the purposes of the HMIS despite fire, flood or other disaster.
- Agencies that are not funded by HUD programs, but utilize HMIS, must comply with the same policies and procedures as Agencies that are funded by HUD.
- Failure to comply may result in termination of the Agency's access to HMIS. Agencies must respond to IHCDA in writing when notified of HMIS Policy Violation within 10 working days of receipt.
    - Agencies should inform IHCDA of how they have responded to the violation.
    - Failure to comply with HMIS requirements may result in IHCDA withholding payments until compliance is complete and documented, or termination of the grant(s).
    - In addition, failure to comply with requirements may result in an agency being ineligible for funding in the next grant year.
- While we use SSL encryption to protect sensitive information online, we also do everything in our power to protect client information off-line.
    - The agency is responsible for ensuring that information that is printed from the HMIS is also kept confidential, private and secure.