SUDS
State Unit Data System

SUDS Tip Sheet: Data Privacy

SUDS data contains both personally identifiable information (PII) and protected health information (PHI), which are protected under the Health Insurance Portability and Accountability Act (HIPAA). All SUDS users are responsible for keeping our clients' data and privacy secure. As more data moves from paper to the cloud, we must ensure data security for the clients we serve.

Authorized Access Only

- SUDS users must apply and pass HIPPA testing before accessing the SUDS system.
- Only authorized users should access SUDS.
- Keep your login information secure, including usernames and passwords.
- NEVER log in using another user's account.
- NEVER give your account information to anyone.
- Lock your devices when away from your desk.
- Avoid using unfamiliar or public Wi-Fi to access sensitive information or log into SUDS.
- If a SUDS user has left your organization, contact the SUDS Help Desk immediately so their account can be closed.
- Notify the SUDS Help Desk immediately if you suspect a data breach or accidental unauthorized access to SUDS data.

Practice "Minimum Necessary"

- Only access the data you need to perform your job.
- Demographic information, including race, ethnicity, gender, living situation, and poverty, should only be reported externally in aggregate.

Follow Encryption Practices

- Any email containing SUDS client data should be encrypted.
- Any emails containing SUDS client data sent to the SUDS Help Desk must also be encrypted.
- Not sure how to encrypt your email? Contact your IT department to learn how.

Remember: CDHS Manages SUDS

- All SUDS users sign a CDHS Application for System Access, which lists the security precautions you must follow as a SUDS user.
- The SUDS Data Team can and will monitor all user activities in SUDS.
- It's the SUDS Data Team's responsibility to ensure that SUDS is used appropriately and that users follow the rules outlined in the application. If users violate rules or expectations or enter fraudulent data, the SUDS team will take steps to secure the system and the data.
- Users who have violated our system rules, like sharing accounts, will receive written notifications regarding any system misuse and will face consequences, including, but not limited to: mandatory training, removal of system permissions, frozen account, and removal from the system. Continued failure to meet systems requirements may result in a corrective action plan for the region's AAA.

The Colorado Department of Human Services (CDHS) is committed to accessibility. For more on CDHS's accessibility policies, please visit Accessibility at CDHS. If you have difficulty using this document's content, please email the State Unit on Aging at cdhs_stateunitonaging@state.co.us or call 303-866-2800.