Recommended Best Practice for Keeping Confidential Information Secure

Implement appropriate safeguards to prevent unauthorized use or disclosure of information:

- Secure information in locked rooms or cabinets
- Do not leave information in places, such as conference rooms, where unauthorized persons could access it
- Do not leave laptops, mobile media devices, cell phones or paper documents in automobiles
- Shred documents with sensitive information instead of throwing them away in the garbage
- Double check fax numbers prior to sending information out; coordinate a system to confirm receipt by the person to whom the information was sent
- Encrypt information sent via email or provide a password protected attachment and send the password in a separate communication
- When possible, use registered mail to send information to confirm it wasn't intercepted or delivered to the wrong party
- Do not store confidential, sensitive, or personal data on non-encrypted laptops or mobile devices
- Do not backup data to non-encrypted media such as diskettes, memory sticks, or CDs
- Ensure agreements with vendors or other contractors include assurances to be HIPPA compliant, if needed , and appropriately protect information to prevent future privacy breaches or security incidents
- Password protect and encrypt all mobile devices
- Keep a log of any breaches and the actions taken
- Develop policies and provide orientation and ongoing refresher training to staff upon hire and at least annually regarding confidentiality. Maintain documentation of each employee's training
- Develop a listing of whom to report a breach, which may be change based on your funding source, report all breaches of SDRC clients to SDRC and DDS
- Assign a security officer to act as "point person" within your agency on confidentiality/security issues
- Complete a security/confidentiality self assessment and have employees sign a confidentiality agreement
- Refrain from public conservations regarding client information. Continuously reinforce and uphold the agency's legal mandates regarding the protection of the confidentiality of client information
- If you have a need for immediate access to client information while out in the field use a portable device that has encryption/password protection or consider using a "travel sheet" which contains very limited, non-identifying information such as clients initials, medication listing, street address, and phone number with no names or social security numbers, etc.
- Assure that home office space used by staff is in compliance with confidentiality requirements
- Determine your agency's HIPPA status and then comply with the rules that apply