CONFIDENTIALITY AND HIPAA

Region V Services believes in and is committed to ensuring that people with disabilities have the right to upmost Confidentiality in all aspects of their lives especially regarding their PHI (Protected Health Information).

The Americans with Disabilities Act of 1990 (ADA) requires medical and disability information to be kept confidential and limits access to those who have a "business need-to-know". (www.halpernadvisors.com)

Region V Services is also mandated by law to follow the rules of HIPAA: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) which regulates healthcare providers' use and disclosure of individually identifiable health information (known as Protected Health Information). Types of PHI information would be a person's last name, address, phone number, why they are receiving services, diagnosis, or medical information including doctor's seen.

Consent is also an important aspect to remember. Consent can be given by the person supported. In the event that a guardian is assigned to a person supported, then consent is given by that guardian. Consent has to be given to share information with other family members that aren't guardians, to provide medical care in general, to attend certain activities, or to have information or photos shared or posted in newspapers, social media, etc. If Region V is not identified as payee for someone receiving services, then consent must also be given to provide assistance with their financial services and needs if any funds are kept by Region V.

There are two main ways to uphold or break Confidentiality, either through verbal or written communication. When thinking about ways to protect people with disabilities confidentiality, the following list provides some tips to remember:

- All confidential documents should be stored in locked file cabinets or rooms accessible only to those who have a business "need-to-know."
- All electronic confidential information should be protected via firewalls, encryption and passwords.
- Employees should clear their desks of any confidential information before going home at the end of the day.
- Employees should refrain from leaving confidential information visible on their computer monitors when they leave their work stations.

- All confidential information, whether contained on written documents or electronically, should be marked as "confidential."
- All confidential information should be disposed of properly (e.g., employees should not print out a confidential document and then throw it away without shredding it first.)
- Limit the acquisition of confidential client data (e.g., social security numbers, bank accounts, or driver's license numbers) unless it is integral to the business transaction and restrict access on a "need-to-know' basis.
- Before disposing of an old computer, use software programs to wipe out the data contained on the computer or have the hard drive destroyed.
- Employees should refrain from discussing confidential information in public places or in front of other people. (www.halpernadvisors.com)

This last statement should be practiced on a daily basis and there are many scenarios to think about when ensuring that a person's confidentiality is being upheld.

For example, not discussing personal information over the phone or in person unless the person is a doctor or other member of the treatment team. These types of people fall into the Relative Confidentially practice of sharing information with others who "need to know this information". In converse, you would not share the same information with a neighbor, friend, or maintenance employee.

Absolute Confidentially is a relationship between two people where no further information can be shared with anyone; for example, a priest or a lawyer. In these situations, there could only be a breach of confidentially if there was a concern of self-harm or concern of abuse and neglect.

Other areas to consider are not gossiping about other staff, other people supported, or family members in front of a person served. It does not matter if the person served is non-verbal, staff should still not discuss other's information in front of them. In these situations, staff can utilize the four skills to assist them in not breaking the Confidentially Policy.

1) You can change the subject
2) Leave the area where the breach is occurring
3) Express concern about the breach and ask them to stop.
4) Consult your supervisor if it doesn't stop or occurs regularly

Confidentiality is vital to providing excellent services to the people we support. All employees are expected to follow these policies even if they leave employment with Region V.

RVS/SD/CH/2/20