Be Safe. Privacy & Compliance in ConnectWellSD

ConnectWellSD
Connect · Collaborate · Empower

This document is designed to help you understand Privacy and Compliance in the ConnectWellSD system so that you can use the system safely and stay in compliance with laws and policy.

Customer Data

ConnectWellSD is capturing customer information from various source systems that was gathered from customers at different times in their life. The data may include self-reported or verified information. System information should be used to start a conversation to further verify the information in ConnectWellSD, and clarify their current status. For quality assurance purposes, additional steps should be taken to validate information in ConnectWellSD.

The information that users see within the customer record will vary based on their department and job. For example, while all users will see demographic information, sensitive customer information such as medical, mental health, and housing will only be seen by workers who need that information to serve the customer.

ConnectWellSD protects information in various ways:

- Access to the ConnectWellSD system is controlled by County single sign-on login and password protection
- You'll only see information that's appropriate to your user role assigned
- ConnectWellSD tracks which user accessed what information and when they accessed it and runs regular audits of user's actions

Entering Data in Customer Records

Users can add information to customer records in open text fields when they create Referrals, Alerts, and Notes on customer records. All users see these open text fields, so be sure to add only factual and observable information that does not violate HIPAA and other guidelines. For example, you may explain that the customer needs translation services, has a mobility issue, or a visual, hearing, or speech impairment. This information can help providers make accommodations.

Do not include any of the following in ConnectWellSD notes: program participation, medical diagnoses, treatment or case notes, prescription drugs, test results, pending applications, pregnancy, etc.

"Practicing" in the System

All information added to ConnectWellSD becomes a permanent part of the system. Do not create practice referrals, form mock CSTs, and do not search for anyone (including yourself!) unless they are a customer to whom you are providing service. If you need practice using the system, contact the ConnectWellSD Support Center (ConnectWellSD.HHSA@sdcounty.ca.gov or (844) 695-5228) to schedule a learning session. This will give you the opportunity to use ConnectWellSD in a practice environment with mock data.

Stay in Compliance

Do's and Don'ts of Compliance:

- Don't go looking for information – do not search for people you know, including but not limited to yourself, family or friends.

- Only search for customers you are working with and have a business need to see their information.
- Never give information from the system to a customer. For example, you would never say, “You live at 1234 Main Street, right?” Instead you might say, “What’s your current address?”
- Don’t share report data with those who don’t have access to the data themselves.
- Lock your screen when you walk away from your computer and be aware of those around you for “shoulder surfing”.
- You, as a county employee, are responsible for keeping customer information confidential and private.

Information is a critical tool that we use to help our customers thrive, but we must remember that customer information viewed in ConnectWellSD is confidential and should not be disclosed to unauthorized persons in keeping with County, State, and Federal laws and policies.

REMEMBER – by signing the CODE OF ETHICS you took responsibility for Confidential Information.

For additional information, visit the HHSA Compliance Office Privacy page and see CAO Admin Manual Policies 0400-01 & 0400-11**.**