

HIPAA



PHI

Health Insurance Portability and Accountability Act

Protected Healthcare Information



AND



1 DO USE A CLO LAPTOP AT A SECURE LOCATION

DO log-on to a CLO laptop at a CLO location. Use the VPN when off site. Be aware of your surroundings and prevent the visibility of your screen when in public spaces or at home.



2 DO SEND SECURE EMAILS

DO share PHI through CLO email if a completed signed release is on file. When sending emails to other authorized persons outside of CLO, encrypt your email by typing: [ENCR] in the subject line before sending an email.



3 DO USE THE LEAST AMOUNT OF PHI INFORMATION

DO share the least amount of PHI necessary when sharing information with authorized persons. If working off-site, carry the least amount of PHI.



4 DO SHARE PHI WITH AUTHORIZED INDIVIDUALS

DO check for authorization before sharing PHI about individuals we serve. Use discretion and be aware of your surroundings when sharing PHI.



5 DO SHARE INFORMATION WITH YOUR TEAM ABOUT INDIVIDUALS WE SERVE

DO share information with your team using a CLO phone, CLO email, or in person.



6 DO PROTECT PHI WHEN OFF-SITE

DO secure and lock-up CLO electronic devices and documents containing PHI when off-site. Keep in a locked briefcase, file cabinet, or office when not using. Keep in the trunk or out of sight location in locked vehicles. Do not leave in vehicles overnight.



1 DON'T USE YOUR PERSONAL PHONE TO TEXT PHI

DON'T use your personal phone to text PHI. This includes pictures, initials, first names, and more. Never use your personal phone to take pictures or make notes on individuals we serve.



2 DON'T USE YOUR PERSONAL EMAIL

DON'T send PHI information on individuals we serve through your personal email.



3 DON'T SHARE PHI WITHOUT A PROPER RELEASE

Before sharing PHI, confirm a proper signed release is on file. When in doubt, fill one out. Always ask permission before taking a picture or sharing PHI even with a release in place.



4 DON'T SHARE PHI WITH ANYONE WHO IS NOT AUTHORIZED

Don't share PHI about individuals we serve with your family members, friends, former co-workers, or any other individual without an authorized release.



5 DON'T SHARE PHI ON PERSONAL SOCIAL MEDIA

DON'T post or message about individuals we serve through personal social media accounts.



6 DON'T LEAVE PHI UNSECURED WHEN OFF-SITE

DON'T leave PHI in unlocked vehicles or unattended in public spaces. DON'T allow friends or family to use electronic work devices. DON'T dispose of PHI in public spaces.



IF YOU SUSPECT THAT THERE HAS BEEN A BREACH OF HIPAA OR HAVE ANY QUESTIONS, YOU SHOULD CONTACT YOUR HIPAA PRIVACY AND SECURITY OFFICER, ABBY FINN EXT. 7210, FOR ASSISTANCE.

Community Living Options would like to remind all team members of the importance of protecting our consumers' information. The Health Insurance Portability and Accountability Act (HIPAA) is a policy that limits how we can store, share, and access consumers Protected Healthcare Information (PHI).

WHAT IS?

PHI

Protected Healthcare Information



Names



Photographs



Birthdates



Addresses



Social Security Numbers



Diagnoses



Phone Numbers



Medications



Health Plan Numbers



Incidents
And More

To protect our consumers, CLO staff should always:

1. Use encrypted emails when discussing consumers with external partners.
2. Always use the least amount of information possible to identify consumers (such as only using initials, not full names).
3. Never send or post photos of our consumers without a proper release in place.
4. Never discuss consumer information with anyone who is not authorized.

As a staff person with CLO, you have access to some of your consumers' PHI and it is your responsibility to protect it. We are continually evaluating the best practices of how to protect this information and expect to have new changes to our policies and procedures to be coming soon.