

TELEHEALTH PRIVACY MEASURES [For The Client](#)

Dr. Jan Martin Dunn, PLLC

LMFT-S, LPC-S, LCDC

13355 Noel Road, Suite 1100

Dallas, Texas 75240

Phone: 214.890.6637

www.drjandunn.com

Some clients feel that they need more privacy/security than other clients require. It is up to you to evaluate your situation and decide what steps you need to take for safety. Following are steps that might be considered/implemented.

It is recommended that you (the client) use the same safety measures that I use for keeping your information confidential.

Paper

It is recommended that you store all paper documents with your information in a locked cabinet.

For same-location (face-to-face) services you may want to turn off any devices location services before coming to the counselor's office.

When receiving Telehealth counseling it is also recommended that you:

- ▶ Conduct the sessions in a private location where others cannot hear you
- ▶ If someone enters your location during the session, acknowledge them so that your counselor will know that there is someone else in the room.
- ▶ Only use devices and internet services that you trust are secure.
- ▶ Password protect your computer, tablet, phone, and any other device with a password that is unique.
- ▶ Use full disk encryption on any computer and/or device you use.
- ▶ Always log out of your sessions.
- ▶ Do not have any software remember your password. Sign in every time.
- ▶ Do not share your passwords with anyone.
- ▶ Do not share your computer when you are logon to any counseling software.

- ▶ If you wish to avoid others knowing that you are receiving counseling services, clear your browser's cache (browsing history), and on your phone, list your therapist by a name rather than as "counselor or therapist."
- ▶ Do not keep your therapist's contact information on your phone if it is synced with other accounts/applications.
- ▶ Have all of your devices set to time out requiring you to sign back in after a set idle time.
- ▶ Keep your computer updated.
- ▶ Use a firewall and antivirus program.
- ▶ Do not record any sessions.
- ▶ Do not download or store information off of your client portal (SimplePractice Web Portal). However, if you do decide to, only store in on an encrypted file.
- ▶ Using secure video conferencing technology (Telehealth By SimplePractice Service)
- ▶ If texting only, use a secure texting application (Signal)
- ▶ Notify you counselor if you suspect any breach in your security.
- ▶ When online, do not login as an administrator.
- ▶ Using your own Router / Access Point
 - Only use a secure network for internet access using a WAP2 security key.
 - Use your own administer ID and password (not the default) for your router or access point.
 - Choose a custom SSID name, not the default name.
 - Limit the range of you Wi-Fi by positioning it near the center of your home.
- ▶ For more information on securing your mobile device visit:
<http://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device>

BY SIGNING BELOW I AM AGREEING THAT I HAVE READ, UNDERSTOOD, AND AGREE TO THE ITEMS CONTAINED IN THIS DOCUMENT.

Signature of Client _____

Printed Name _____

Parent/Guardian Signature _____

Date _____

TELEHEALTH PRIVACY MEASURES For The Client

