SECURITY CHECKLIST FOR ELECTRONIC DEVICES

Here are some "HIPAA-friendly" security measures for your computer and smartphone. For more detailed information on HIPAA security compliance, risk assessment, and breach notifications, visit your professional organization's licensing board or membership websites.

Security Settings

- ✓ **Full-device or full-disk encryption:** By scrambling (encrypting) your data before it gets written onto your device's hard drive, the information becomes invulnerable to confidentiality breaches if your device is ever lost or stolen. For instructions and more details, visit https://spreadprivacy.com/how-to-encrypt-devices/ and https://www.wired.com/story/encrypt-all-of-the-things/

- ✓ **A strong password**: A strong device password is necessary for the encryption process. Strong passwords should consist of upper- and lowercase letters, as well as at least one numeral and/or symbol. For tips, see this CNet article: https://www.cnet.com/how-to/strong-passwords-9-rules-to-help-you-make-and-remember-your-login-credentials/

- ✓ **Antivirus/anti-malware software**: Make sure you have antivirus software updated and running each day. Popular products include Norton, McAfee, and Malwarebytes. *PC Magazine* published its top picks at https://www.pcmag.com/picks/the-best-antivirus-protection

- ✓ **Active firewall**: Firewall software serves as your computer's gatekeeper, filtering traffic and blocking unauthorized access to the private data on your computer. It can also help block malicious software from infecting your computer. Make sure your device has its firewall turned on (for instance Windows 10 includes Microsoft Defender Firewall), or that your antivirus protection software includes firewall protection.

- ✓ **Automatic logout or lockout:** Set your device's security options so that it locks you out after a short period of inactivity. This ensures unauthorized users will not have access to your programs and files when you leave your phone or computer unattended.

Maintenance Tasks

- ✓ **Backup your files**: If your client information is only stored on a single device and is not accessed elsewhere, that information needs to be backed up. If you perform backups using an external hard drive or USB/thumb drive, remember to encrypt it. It is also important to have your computer and backup stored in two different locations (for instance, storing your computer at home and your backup at your office).

- ✓ **Update your OS (operating system) software:** By keeping your device's software updated with the latest patches and fixes, you will be protected from new security issues that develop.

- ✓ **Beware of data syncing**: To make your life easier, your devices synchronize your app data for you: Apple syncs to your iCloud, and Android and Chrome sync to Google. However, this convenience becomes a security risk when stored client information is sent to Apple servers, Google servers, or Microsoft servers without the HIPAA-required Business Associate Agreements (BAAs). You can either change the settings on your devices so they no longer sync to apps that handle your client information, or you can download the server's BAA.

- ✓ **Create a separate user account for your practice:** By creating a separate user account on your computer for your therapy practice, you can prevent potential security errors or breaches to your client's identity and personal information.