Fresh Air Counseling
Breathe. Be

Kelly K Jerome, MS, LPCA, NCC, CRC, CCTP

919.533.9377 | kjerome@fresh-aircounseling.com

Electronic Records Disclosure

I keep and store records for each client in a record-keeping and practice management system hosted by TheraNest. Here are ways security of your records are maintained:

- TheraNest is HIPAA compliant. All data is encrypted and stored securely using Amazon Web Services. Amazon's servers infrastructure are certified, ensure the highest physical security and guarantee a 99.9% uptime. You can read more at https://aws.amazon.com/compliance. Amazon Web Services are also HIPAA, and SOC compliant. AWS has achieved ISO 27001 certification and is a Level 1 service provider under the PCI DSS standards We perform continuous data backups and snapshots. All data in TheraNest are also encrypted using SSL in transit, and encrypted at rest. TheraNest limits access to "protected health information"(PHI) in accordance with HIPAA. TheraNest's workforce members are trained on the privacy and security requirements applicable to protected health information, and TheraNest's "business associates" are required, pursuant to the terms of their agreements with us, to implement required safeguards.

I may store some records in a system produced and maintained by Google (G Suite). This system is "cloud-based," meaning the records are stored on servers which are connected to the Internet.

Here are the ways in which the security of these records is maintained:

• I have entered into a HIPAA Business Associate Agreement (BAA) with Google. Because of this agreement, Google is obligated by federal law to protect these records from unauthorized use or disclosure. This BAA covers: 1) Records and file storage 2) Email kjerome@fresh-aircounseling.com 3) Forms found on my website

• The computers on which these records are stored are kept in secure data centers, where various physical security measures are used to maintain the protection of the computers from physical access by unauthorized persons.

• Google employs various technical security measures to maintain the protection of these records from unauthorized use or disclosure.

o From their website: "In addition to supporting HIPAA compliance, the G Suite Core Services are audited using industry standards such as ISO 27001, ISO 27017, ISO 27018, and SOC 2 and SOC 3 Type II audits, which are the most widely recognized, internationally accepted independent security compliance audits. To make it easier for everyone to verify our security, we've published our ISO 27001 certificate and SOC3 audit report on our Google Enterprise security page."

• I have my own security measures for protecting the devices that I use to access these records: 1) On computers, I employ firewalls, antivirus software, passwords, and disk encryption to protect the

computer from unauthorized access and thus to protect the records from unauthorized access. 2) With mobile devices, I use passwords, remote tracking, and remote wipe to maintain the security of the device and prevent unauthorized persons from using it to access my records.

Here are things to keep in mind about my record-keeping system:

• While my record-keeping company, TheraNest, and I both use security measures to protect these records, their security cannot be guaranteed. TheraNest keeps a log of my transactions with the system for various purposes, including maintaining the integrity of the records and allowing for security audits. These transactions are kept for six months. Some workforce members at Google or TheraNest, such as engineers or administrators, may have the ability to access these records for the purpose of maintaining the system itself. As a HIPAA Business Associate, Google is obligated by law to train their staff on the proper maintenance of confidential records and to prevent misuse or unauthorized disclosure of these records. This protection cannot be guaranteed, however.