Christo Franklin, Psy.D, M.Div., psy24447
(310) 863-6199
520 S. Grand Ave., Ste 680 L.A., CA 90071

This document explains Dr. Franklin's Security Policy and he is required to give it to you by a federal law call the Health Information Privacy and Portability Act (HIPAA). The purpose of this law (and of the California Board of Psychology interpretation of this law) is to require Dr. Franklin to tell you how Dr. Franklin will make certain, in 18 steps, that no unauthorized person has access to information about you that is protected by HIPAA.

1. Assigned Security Responsibility: In Dr. Franklin's clinical psychology practice, John Salatti, JD, is the HIPAA Security Officer who is responsible for developing and implementing security protocols and who can answer your questions about how your information is being protected. You are never charged for his time to answer your questions about how he is protecting your information; it is your right to ask him to explain.
2. Security Management Process: As HIPAA Security Officer, Mr. Salatti personally reviews his practices designed to prevent, detect, contain, and correct HIPAA violations, every 6 months, September 1 and March 1. He attends trainings about security and technology relevant to HIPAA compliance. And he consults with other clinical psychologists about how they ensure patients' or consultees' information's security.
3. Workforce Security: Dr. Franklin's employees who have access to any protected information receive training and supervision to ensure their compliance with data security.
4. Information Access Management: Dr. Franklin keeps information on a hard drive that is encrypted and on a Google enterprise account in the cloud, which is also encrypted.
5. Security Awareness and Training: Mr. Salatti trains employees about HIPAA compliance.
6. Security Incident Procedures: If Dr. Franklin believes there is reason to suspect someone or some bad computer program has stolen information about you, he will call you to tell you about it so that you can decide what you might need to do, such as change your credit card number or bank account number. If a fire, earthquake, or other natural disaster destroys the building where his computer is and he can't find the computer, he will try to tell you as soon as the telephone system is working.
7. Contingency Plan: Dr. Franklin keeps one copy of your information on his SImplePractice.com account (a secure, cloud-based documentation service for psychotherapists), some parts of records related to your case are stored in cyberspace, such as Google Drive, where it is securely encrypted in compliance with HIPAA, and there is an encrypted, external hard drive copy as well.
8. Evaluation: Dr. Franklin and Mr. Salatti attend special trainings and also describes to colleagues and to his professional association what measures he is taking so that they can tell him how to improve.
9. Business Associate Contracts: Dr. Franklin requires all business associates (answering services, billing services, shredding services, computer technicians,

etc.) to put in writing that they are trained properly and in compliance with HIPAA security rules.

10 Workstation Use: No one else but Dr. Franklin and his employees has a key to where he stores his computer and encrypted, external hard drive.

11 Workstation Security: All Dr. Franklin's employees' computers require re-login, using a password for encryption, if there is no user activity on that computer.

12 Device and Media Control: Dr. Franklin has an encrypted backup drive that is locked in a metal file cabinet. Before disposing of a computer, Dr. Franklin uses a professional company specializing in erasing patient or consultee information according to HIPAA standards of security.

13 Access Controls: Dr. Franklin will ensure only appropriate users have access to your electronically stored information.

14 Audit Controls: Dr. Franklin will use software to protect and detect the security of his computer files, and to notify him of attempts by unauthorized persons to get copies.

15 Integrity: Dr. Franklin is still researching software that will ensure records remain unaltered.

16 Person or Entity Authentication: Dr. Franklin uses a password both to access his computer and a second password to encode any protected information about you that is stored in the cloud or on the backup drive.

17 Transmission Security: Dr. Franklin uses Google enterprise level encryption which encrypts emails that are sent, and stores them in an encrypted cloud archive.