



Notice of Privacy Practices for Protected Health Information (PHI & ePHI)

**THIS NOTICE DESCRIBES NOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.**

**PLEASE REVIEW IT CAREFULLY.**

### **General Information**

The protection of your health information is very important. As a mental health professional I recognize that many of the things we discuss are sensitive, and because of this it is important that you are aware of how this information is used and may be revealed. This document contains a description about how your protected health information is used and sometimes disclosed. As a healthcare professional covered under the federal “HIPAA” law I am required to give you this notice and to abide by its terms. (I reserve the right to change the terms of this notice, and if that happens I will provide you with an updated copy with the changes.)

In general, the communications between a patient and psychologist are confidential and protected by law and I can only release your protected health information with your permission, or under certain circumstances. This document and the other intake documents you received discuss those circumstances. When I make a disclosure, I will always try to limit the information that I reveal. In general, I will try to disclose only the amount necessary.

### **Electronic Records and Electronic Protected Health Information (ePHI)**

The HIPAA Privacy Rule protects the privacy of individually identifiable health information, called protected health information (PHI), as explained in the Privacy Rule. The Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form. The Security Rule calls this information “electronic protected health information” (e-PHI). The Security Rule does not apply to PHI transmitted orally or in writing.

Electronic records are subject to similar concerns and requirements as paper records. I keep electronic medical records on each patient. The 2005 HIPAA Security Rule provides specific guidance on managing electronic protected health information. It applies to practitioners who must comply with HIPAA and who store or transmit such information. The rule requires that I take special care in maintaining electronic records and that I conduct a risk analysis of specified issues and security measures appropriate for the practice. The electronic practice management company that I use takes reasonable efforts to maintain their service in a manner that includes appropriate administrative, technical and physical security measures designed to protect the confidentiality, availability and integrity of ePHI as required by HIPAA.

The database is fully encrypted, access to the application is encrypted, data is backed up regularly at a SAS 70 Type II certified data center, strong passwords are required and changed frequently, all actions are logged which offers a strong audit trail, powerful firewalls protect the servers, allows ability to print a paper copy of medical file, and limited IP addresses are allowed to access the service.

I make reasonable and appropriate administrative, technical, and physical safeguards for protecting ePHI.

Including: (1) Ensuring the confidentiality, integrity, and availability of all e-PHI that I create, receive, maintain or transmit; (2) Identifying and protecting against reasonably anticipated threats to the security or integrity of the information; (3) Protecting against reasonably anticipated, impermissible uses or disclosures; and (3) Ensuring compliance by my workforce.