# Security Policy Regarding Electronic Information

## Lawrence E. Hedges, Ph.D., Psy.D., ABPP

Electronic transmission and storage of confidential information always entails security risks. This office, following HIPPA (the 1996 Federal Health Information Portability and Privacy Act), has adopted the following security standards.

I. Administrative Standards:

1. Assigned Security Responsibility: Dr. Lawrence Hedges is the security officer responsible for developing and implementing security protocols and answering questions.

2. Security Management Process: Dr. Hedges continuously monitors all areas of electronic storage and transmission throughout the office and at backup storage sites in order to prevent, detect, contain, and correct any violations.

3. Workforce Security: The security officer has created a system that insures and limits appropriate employee access to EPHI (Electronic Personal Health Information).

4. Information Access Management: A system of passwords has been created that guarantees that only authorized people have access to each type of client information—i.e., notes, charts, and billing information.

5. Security Awareness and Training: At the commencement of employment and then again every January all employees who have any access to EPHI are trained in HIPPA Privacy and Security protocols.

6. Security Incident Procedures: Any breaches in EPH security that are detected will be promptly corrected and disciplinary actions taken. In the event of a security breach action will be taken by Dr. Hedges to correct the breach and, when appropriate, to notify promptly any people whose confidentiality may have been compromised.

7. Contingency Plan: All EPHI are secured with locks and passwords and backed up in separate locations in the event of theft, vandalism, fire, or natural disaster.

8. Evaluation: Every January and at any other appropriate time there is a full staff review of Privacy and Security Policies and Practices.

9. Business Associate Contracts: Dr. Hedges maintains contracts with all business associates who in any way ever have access to EPHI, thereby insuring their compliance with HIPPA Privacy and Security Standards—at present only our computer technician.

II. Physical Standards

1. Facility Access Controls: All EPHI is stored in locked rooms and/or locked file cabinets.

2. Workstation Use: Each workstation can only be accessed by appropriately authorized personnel.

3. Workstation Security: All devices are secured against use by or removal by unauthorized personnel.

4. Device and Media Control: When devices and media are being transported they are secured in locked trunks. When being discarded wipe-it software is used to insure complete erasure.

III. Technical Standards

1. Access Controls: Protocols allow only appropriate access to authorized users.

2. Audit Controls: Ongoing monitoring by Dr. Hedges of all procedures and practices locates any possible breaches.

3. Integrity: Backup files on alternate sites insures against improper alteration or destruction of EPHI.

4. Person or Entity Authentication: Only authorized personnel have the several building and room keys plus the required passwords to EPHI.

5. Transmission Security: Any PHI that is being transmitted over an electronic transmissions network is encrypted. Norton security software has firewalls against viruses and hackers.

Signature_____Date_____

Print Name: _____