# PASTORAL COUNSELING ASSOCIATES OF PORTLAND, P.C.
# POLICY FOR PROTECTING CLIENT PRIVACY

It is the policy of Pastoral Counseling Associates of Portland, P.C. to comply with the Health Insurance Portability and Accountability Act of 1996 by implementing the applicable regulations of the United States Department of Health and Human Services. In the event that Oregon provides greater protection and rights, Oregon's laws and regulations are noted in the procedures and followed.

This policy and its procedures do not attempt to cover everything in the government's privacy rules. If any client, employee, business associate, other member of our workforce, or member of our Board of Directors has questions about their responsibilities surrounding a client's health information privacy, they should take them to the HIPAA Compliance Officer (HCO).

The "client" includes prospective clients, current clients, former clients, and/or their authorized representatives.

All of our employees, business associates, other members of our workforce, and the members of our Board are expected to be in compliance with this policy and its procedures at all times. Failure to comply can result in disciplinary action, up to and including the termination of their affiliation with us.

## PROCEDURES FOR PROTECTING CLIENT PRIVACY

1. Client information of any kind is stored under lock and key in a space dedicated exclusively to client information.

2. Telephones over which a client might in any way be referenced are well out of the hearing range of any person not authorized to hear those references.

3. When client records are out of storage and in use, their contents are protected from unauthorized viewers at all times.

4. Any reference to a client appearing on a computer screen, paper document, chalk/dry erase board, telephone message form, task list, appointment books, palm pilots, etc. is protected from unauthorized viewers at all times.

5. We refrain from making any reference to a client over a cell phone or other wireless telephone technology.

6. All voice mails, or any recorded messages referencing clients are protected from unauthorized listeners at all times.

7. The fax machine over which any clients may be referenced is protected from unauthorized viewers at all times.

8. All out-going faxes referencing clients have a cover sheet with a confidentiality statement directed to unauthorized viewers.

9. Every room in which client information is kept has a lock on the door.

10. Every computer in which any reference to a client might be found has a password to access its files.

11. Individual computer passwords are known only to the person(s) authorized to see/access any client information in that computer.

12. Each computer's password is written on a sheet of paper, sealed in an individual envelope and stored in a secure, locked, fireproof place to be accessed only by the HCO and Executive Director in the event of a HIPAA complaint and the authorized person's unavailability.

13. All information about a client is kept secure by the authorized person even when being used, and especially when left unattended momentarily.

14. Any information in any form (paper, electronic, and even appointment books, palm pilots, etc.) about a client conforms to all security procedures when that information is off site.

15. When transporting any information about a client, it is stored in a secure, locked container dedicated only to client information that also has information inside warning unauthorized viewers of the confidential nature of the material and instructions for its return.

16. All computers containing any client information have appropriate security measures (firewalls and encryption) to guard against "hacking" or any other form of unauthorized access.

17. All paper documents containing any client information are immediately shredded after they are no longer needed.

18. All electronic records containing any client information are immediately deleted from the hard drive and/or other storage locations after they are no longer needed.

19. All software venders have attested in some written format that computer software packages are HIPAA compliant.

20. All soft/hardware application service providers (ASP's) have attested in some written format that they meet HIPAA security standards.

21. All third party payers (insurance, managed care, employee assistance, congregational assistance, etc.) have attested in some written format that they are HIPAA compliant.

22. All email containing client information (including to or from the client), is encrypted.

23. When any information about a client is provided to anyone, it is determined whether they are authorized to have that information and a log of each authorized provision is kept.

24. When business associates (BA's) have access to any information about a client, they are HIPAA compliant.

25. All verbal conversations about a client are held around or with only those authorized to hear that information.