Peace of Mind Counseling

HIPAA Compliance Manual

Table of Contents

Appendix

Compliance Forms and Logs

Compliance Officer Training

Monitoring Compliance Procedure and Logs

Restriction of PHI Disclosure

Risk Assessment Form

Introduction

In 1996, the United States Congress enacted the Health Insurance Portability and Accountability Act (HIPAA). HIPAA was designed to accomplish a number of objectives, one of which is to protect the privacy of individually identifiable health information. Protection standards exist for protected health information (PHI) in all forms, including electronic formats (ePHI).

The standards set forth by HIPAA apply to "covered entities," including mental health care providers and the offices in which they work. Peace of Mind Counseling is a covered entity and is required to comply with the HIPAA regulations.

This manual details the policies and procedures established for Peace of Mind Counseling to ensure HIPAA compliance. Its contents include the procedures as spelled out in the HITECH update (2009) and the "Final Rules" update which became effective March 26, 2013 and was to be in place in the covered offices by September 23, 2013. It should be noted that while this manual contains the rules and regulations of HIPAA, if the state law is more constricting than the HIPAA law, the more constricting law applies.

Chapter 1: Policies and Procedures

We need to address the safeguards in three areas of the office. They are the administrative, physical and technical areas.

Administrative Safeguards

Administrative safeguards refer to the policies and procedures used by the staff of Peace of Mind Counseling clinic to comply with HIPAA standards.

Training Program

All clinic personnel are required to participate in a formal HIPAA training program. All staff will receive the training within 30 days of their start of work with Peace of Mind Counseling.

The training involves watching and listening to the HIPAA materials on the Therapist Consultant's website and then taking the HIPAA Training Quiz. Successful completion of the training and quiz is required in order to work in the clinic. Ron Haynes &/or Otis Whigham will go over any items that the new staff had missed on the test. Anyone receiving a grade less than 82% on the quiz must repeat the training.

Additionally, staff will be told where this manual is kept so that they can refer to it as needed.

Documentation of Training

Training of clinic personnel will be recorded in the HIPAA Training Log found in the back of this book.

HIPAA Notification

All clients who receive services in the clinic are given a HIPAA Privacy Policies document before their first visit (see Appendix A). They sign the Acknowledgement of Receipt of Notice of Privacy Practice form indicating that they received the notification. A HIPAA Privacy Policies document is also posted in the reception room of the clinic and on the Peace of Mind Counseling website.

Release of Information

Client PHI is typically released to another party only when the release is requested, in writing, by the client or client's legal guardian. A "Release of Medical Information" form is completed when a request is made (see Appendix B).

PHI may, at times, be release without client authorization (for example it can be released to health oversight agencies), but only in accordance with strict policies and according to law. However, with a few exceptions, psychotherapy notes do not have to be released. Psychotherapy notes do not have to be released even to the patient.

A therapist cannot coerce the patient into releasing his personal file by telling the patient that she will treat the patient only if she (the therapist) is allowed to release the notes.

There are certain times when the release of information is required by law. They include:

1. Child abuse and neglect

2. Court orders

3. Subpoenas (in only some cases and some states)

4. Threats of physical violence or danger

In general, PHI cannot be released to family members of an individual without the individual information.

Type Classification

The professionals and staff that work at Peace of Mind Counseling will be classified by type.

Type I: This person has complete access to PHI.

Type II: This person is someone who directly assists a type I worker.

Type III: This person has access to just summary information and demographic information and such other information as needed to perform their job.

Type IV: This person has access only to information that a type I person has agreed to in writing.

Type V: This person will have no direct access to PHI.

Peace of Mind Counseling employees must take every precaution to release only the minimum amount of information necessary to accomplish the tasks for which the information was requested. The amount of information released will be relative to the task to be completed and relative to those requesting the release of information.

Patient's Rights Regarding PHI

Patients have certain rights regarding the control and content of their PHI. They have the following rights:

1. They have the right to see their PHI (with the exception of their psychotherapy notes)

2. They have a right to a copy of their PHI.

3. They have the right to request an amendment to the records. The therapist, however, can deny the request to have the records amended. In that case, the parties must go through mediation procedures.

4. They have a right to an accounting of the disclosure of their records.

5. They have a restricted right to restrict any PHI to health plans or insurers if the patient is paid for their own care. There is a form in the back of this manual that is filled out by the patient who wants to restrict personal records release.

The therapist can release a patient PHI in limited amounts to another provider for emergency health treatment.

Ensuring that Disclosures are the Minimum Necessary

When a request is received to disclose PHI, the request is reviewed by the office manager and only the minimum necessary amount of information will be disclosed.

Peace of Mind Counseling will not release any information to any institution or organization for fundraising purposes. In addition, Peace of Mind Counseling will not use patient information for marketing purposes nor will Peace of Mind Counseling sell patient information – even with the patients consent.

Accounting for Disclosures

The clinic staff will keep a copy of the Release of Medical Information form in the patient's folder. In keeping with HIPAA Privacy Rules, the form specifies who has received access to the client's PHI and ePHI.

Requests for File Review and Copy

Clients who have records in the clinic may ask to see/receive a copy of their PHI. The request must be made in writing, and will be fulfilled within 30 days of receipt or 60 days if the records are stored off site. Note, however, that HIPAA does not allow clients to have access to their Psychotherapy Notes.

Requests to Amend a Record

Clients have the right to amend their record if they believe the record is incomplete or not accurate. The amendment will become part of their ongoing file. Requests for record amendments must be made in writing. Clients may not delete any prior information or part of the Record and may not change or delete any diagnosis.

Security Assessment

Ron Haynes &/or Otis Whigham, our security officers, will conduct an annual assessment of the clinic's compliance to the policies described in this manual. As part of the annual assessment, the administrative and clinical staff will be asked to search the clinic for any potential security problems and to recommend additional security measures.

Reporting of Security Violations

Clinic personnel are required to report any potential violations of HIPAA to Ron Haynes &/or Otis Whigham.

Responding to Violations and Preventing Further Violations

When potential problems are reported or discovered, Ron Haynes &/or Otis Whigham will investigate the situation and complete a Security Incident Report (see Appendix D). They will then take appropriate corrective measures to help ensure that this violation does not occur again. Corrective measures may include personnel re-education, dismissal of offending staff, policy revision, building modification, and/or equipment positioning or alteration.

Policies and Procedures to Access Protected Health Information

Access to PHI is limited to clinic personnel and business associates. Only the information needed is released.

Business Associates

"Business Associates" are any third party who provides services to the clinic and in so doing may have access to PHI. Financial institutions and simple business conduits such as the post office are not considered Business Associates. Also, parties who have no access to PHI like janitors and maintenance people are not required to sign a Business Associates Agreement. In the event the clinic enters into an arrangement with a business associate a Business Associate Agreements will be utilized.

Physical Safeguards

Physical safeguards refer to the ways in which Peace of Mind Counseling controls physical access to protected information.

Building Access

Access to the clinic is limited to clinic personnel. Keys are dispersed by Ron Haynes &/or Otis Whigham, who maintain a record of key distribution. Keys are returned to them upon termination from clinic. All PHI is stored either in the Receptionist area or each respective counselor's office. Peace of Mind Counseling uses security locks, certain ones of which are keyed only by the respective clinicians and Breakthrough staff. The receptionist area is usually locked when there is no receptionist on duty.

Documentation

Session notes are recorded through Practice Fusion, a secure electronic medical records system. The clinic staff stores their notes on that system.

Document Retention

Electronic medical records are retained for 7 years. Paper files of clients are stored in locked file cabinets.

Document Disposal

Client paper files are maintained for 7 years after the patient terminates/is terminated from care. After that period, the file content is shredded.

Work Stations

Computer screens are not in direct view of unauthorized persons.

Technical Safeguards

Technical safeguards refer to the ways in which Peace of Mind Counseling controls access to computer systems and protects communications containing PHI transmitted electronically from being intercepted by anyone other than the intended recipient.

Electronic Medical Records System

The clinic uses Practice Fusion, an electronic medical records system designed specifically for health care practices. Practice Fusion can only be accessed by clinic personnel, each of which has a unique user name and password. Access is

further restricted by safety measures in the system that keep users from being able to view records of clients who are not their own.

Computer Workstations

The computers in the clinic are turned off after business hours. All clinic staff/clinicians log off of Practice Fusion and other documents before leaving.

Computer Backup

PHI is backed up/stored on respective clinician's hard drive kept in their office computers.

Faxing

The FAX machine in the clinic is located in receptionist and is checked throughout the day to ensure that faxed documents are not left unattended. The office containing the FAX machine is locked when the clinic is not open.

If faxing, only the PHI actually needed is sent, and a cover letter with a confidentiality statement accompanies the information to help prevent casual reading.

Emailing

The emailing of client information is done using Microsoft 365 Business Version which is HIPAA compliant.

Texting

If texting is done it is through Outlook with Microsoft 365 to maintain HIPAA compliance.

Telephoning

Calls are made to clients from the receptionist area only for routine appointment reminders and appointment clarification. Only first names are used. Calls to

clients that require more disclosure of information are made from the phones in the private offices.

Data Maintenance and Emergency Procedures

Since January of 2012, most private health information in the clinic is ePHI that is maintained by an Electronic Medical Records System (Practice Fusion). All other PHI is kept in locked metal file cabinets and filed away. In the event of a disaster or damage to these records every effort will be made to restore the lost or damaged data as shown in the chapter on contingency planning.

Chapter 2: Security Officers

Ron Haynes and Otis Whigham will function as both the security officers and the privacy officer. The staff will be informed of their role as security officers and privacy officers.

Their duties will include:

1. Manage the implementation of the omnibus rules program

2. Report to management on a regular basis regarding the implementation of compliance procedures

3. Create and maintain a compliance training program for employees

4. Provide agreements for business Associates and maintain their files

5. Act on matters of potential noncompliance

6. Report all breaches of more than a “low probability”

7. Place a written document explaining each breach in the back of this manual

8. Take corrective action with all employees

9. Develop new programs and policies to help protect PHI. If they need outside help to conduct a security risk assessment they have the power to employ a nonbiased party to assist in assessment.

They are responsible for knowing HIPAA regulations, training the clinic staff in HIPAA compliance, and assuring that HIPAA-related policies and procedures are instituted and followed. They will:

- Update HIPAA policies and procedures and place them in this manual.
- Oversee the implementation of the policies and procedures contained in this Manual.
- Ensure that all clinic personnel are trained according to HIPAA and the policies and procedures of the clinic.
- Review activity that takes place in the clinic to detect security risks.
- Investigate and respond to potential security breaches and take appropriate action in the event of a breach in security, and eliminate or mitigate any damaging effects.

Chapter 3: Security Risk Assessment

Each year during the month of December we will conducted a security risk assessment. We will also perform a security risk assessment if we find that there has been an actual or potential security breach.

We will assess the security risk by looking at the administrative, physical and technical safeguards from an information standpoint. We will review the security assignments, training the staff regarding security assignments, review any incidents of potential violations that have been reported during the year and ensure that all necessary business associate agreements have been used.

From the physical safeguards perspective, we will evaluate the physical access to patient records, positioning of workstation, workstation security.

From a technical safeguards perspective, we will evaluate transmission security and other technical security issues and media control such as texting, and e-mail and phone calling.

In keeping with Meaningful Use Core Measure 15, we annually review the security and procedure of our electronic health records filing and storage. We will also

conduct a Security Risk Analysis. Corrective action will be agreed upon by our compliance officers and the owners of the clinic.

Chapter 4: Procedures to Manage Potential Risk

Improper training of the staff is one of the biggest concerns in handling potential risk. As a result we will have annual training and testing of our employees as well as training of new staff within 30 days of joining our office.

We will also review our means of sending electronic data to make sure that no non-compliant sources such as g-mail, ATT, and Sprint are not used and that we are continuing to correctly use Vsee and Microsoft 365 compliant software when communicating ePHI.

We have computer battery supply to protect data during an electrical outage and, again, we will keep our business associate agreements up to date and compliance manuals current and available to employees.

Chapter 5: Staff Training

Each year, during the month of December, our compliance officers and our clinicians will review our compliance training which will include a discussion of any security risks.

Peace of Mind Counseling will, on an annual basis, provide employee training which among other things will include the following topics:

1. The definition of privacy, security, PHI, EH R, ePHI, covered entities, business Associates, conduits and penalties.

2. Our position on using patient information to raise funds through marketing and our position on having our office do research using patient data.
3. Restrictions on use of social media
4. A review of the compliance manual
5. New forms including notice of privacy practices and business associate agreements.
6. Working with our security officers
7. Limiting the amount of information released on patients by the clinic
8. Breach reporting plan

While training the staff we will ensure that each staff member understands the importance of compliance, that each staff person who has access to PHI has their own username and password, and review of the policy and procedures. We will also remind the staff that they cannot use their personal electronic devices to store or transmit ePHI or take it outside the office. Staff will be tested after their compliance training and shall receive an 82% or better score to pass the test. Anyone who does not pass the test will be retrained on the lacking areas and retested.

Manual Update. We will also spend this time updating the compliance manual with the information from our office and facility.

Chapter 6: Business Associates

During the same time we will review all business associate agreements for accuracy and determine if other business associate agreements should be signed. We will review to determine if we have omitted any businesses that need to sign a business associate agreement. We will store all our business associate agreements in the back of the compliance manual found in the top cabinet in the conference room.

Determination of Need. At the end of this security risk assessment we will determine if there is a need to change and update any procedures to improve compliance.

Chapter 7: Employee Termination

Regardless of whether the employee termination is voluntary or involuntary the following procedures must be followed:

1. Return of the employee's office keys.

2. Returned of any equipment used by the employee.

3. Remind the employee of the privacy policies they agreed to.

4. Change the front door lock.

Chapter 8: Breach and Sanction Policy

Anytime there is a potential breach of confidentiality it should be addressed by the security officers. To determine if a breach has occurred and to determine if that breach should be reported to HHS, you should use the following procedure:

1. Decide if the event was an actual violation of the privacy rule.

2. Decide if the event falls within any exclusions to the privacy rule.

3. Conduct a risk assessment. According to the Department of Health and Human Services, the following factors should be considered in any risk assessment of a potential HITECH breach. Covered entities should evaluate the type of PHI involved in the potential breach. The more sensitive or private information, the more this factor weighs in favor of a reportable breach. For example if individuals name is disclosed and the fact that he/she received unspecified services a general hospital, this risk may be low. However, if the information indicates the type of services received or that the services were provided by specialized facility, this increases the risk of harm.

To determine the amount of risk you must also consider:

1. The persons involved-if the information was sent to another healthcare entity the risk is lower.

2. Actual acquisition or viewing of PHI. It is possible that the PHI can be returned prior to opening or reading the PHI.

3. Steps taken to mitigate. Practitioners may be able to take immediate steps to mitigate an impermissible use or disclosure.

4. Ask if only patient information was disclosed. If non patient information was also disclosed the risk is lower.

We will use the risk assessment guide found in the back of this manual to help assess risk.

Low risk breaches do not have to be reported.

Each security violation or potential violation will be dealt with in full detail. If there has been a security breach we will sanction the employee in one or more of the following ways:

1. Require more training. If it appears that the breach was due to lack of training and if it was unintentional, it may only require corrective action and additional training.

2. Remove the employee from that responsibility. If it appears that the employee is incapable of doing a certain task involving PHI, that employee will be removed from that duty.

3. We will assess what lead to the breach and put in place a procedure to review the employee's future activities of similar nature.

4. Discipline the employee. If the breach was because of carelessness the employee will be terminated or disciplined.

5. Terminate the employee. For a severe breach or one of intent, the employee will be terminated.

Reporting a Security Breach.

Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

- **Media Notice**

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

- **Notice to the Secretary**

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the HHS Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60

days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

Peace of Mind Counseling will not retaliate with employees who report a potential privacy breach and employees will not be intimidated in any way. Either potential intimidation or retaliation should be reported to the security officer.

Once a breach has been identified, Peace of Mind Counseling will work to mitigate the circumstance or procedure. They will do this in the following way:

1. Put in place appropriate and reasonable administrative technical and physical safeguards to protect, in the future, the privacy which was breached.

2. Retrain personnel as needed.

3. Change policies and procedures to address the violation in such a way that it prevents further violations from occurring.

4. Document the changes that have been made.

Chapter 9: ePHI System Device Inventory and Retirement

Devices Inventory

This systems and devices inventory will include, cell phones, laptops, tablets, iPads (or similar), desktop computers, fax machines, terminal server, backup devices and any other storage or transmission devices. We will note where they are located and who they are assigned to and their usage.

Virus Protection

Peace of Mind Counseling protects their computer system from viruses and malware's by using various anti-virus software, such as McAfee.

Retiring Devices

Peace of Mind Counseling disposes of their old computers and other electronic storage devices in the following way:

1. All patient information is removed from the device's storage.
2. The device is taken out of service and stored in locked room areas until they can be professionally destroyed by IT safety specialists.
3. Those portions of the device that are not capable of storage (such as computer screens) are disposed of by regular means.
4. The information storage components of the device will be serviced by IT safety specialists, and any potential data will be professionally destroyed.

Chapter 10: Workstation Inventory

We will maintain a list of where we have computers and who they are assigned to and what they are used for. This list will be kept in the back of the main HIPAA compliance manual which is kept by the compliance officers. The list will be updated on a regular basis as new equipment is added and at the end of the year.

Chapter 11: Written Policy and Procedure

We have the following policies and procedures regarding how to deal with security issues.

1. Employees shall not share passwords or use each other's passwords or usernames.
2. Employees should not use another employee's workstation on a regular basis.
3. Employees shall have strong passwords that include special characters and upper case and lower case letters.
4. Your password should never be shared.
5. Your password should be changed frequently.
6. We will follow the "Minimum Necessary Rule" and provide outside sources only the information necessary to transact the required procedures.

Chap 12: Written Procedures Supporting Policy

We have established office policies set up specifically to guard PHI. These policies are enumerated below. We will review these policies each December to assure that they are still in place and being followed.

1. Sound blockers may be utilized.

2. When possible we avoid addressing the patient by name in any public area such as the reception area of the clinic. When a patient is addressed by name we use first name only.

3. We play background music and/or video music in the reception room as a "white noise" barrier.

4. We established a policy that does not allow the reception room doors to be propped open.

5. We positioned any computers in the receptionist area so that they cannot be seen by patients or other visitors.

6. We do not allow patient files or any other identifying information to lie in the receptionist area at any time. Temporary files are laid face down.

7. The door between the receptionist area and the common hallway is to remain closed and locked after hours.

8. Inside the respective clinicians' offices, file cabinets are always locked when not in use.

9. In the counseling rooms we have placed the workstations so that they cannot be seen by patients or people other than the therapists when entering or exiting the counseling room.

10. We have screensavers that automatically activate after a short period of time.

11. Each therapist and clinical staff worker has their own username and passwords.

12. Our facility is designed so that patients or other visitors to the clinic can use restroom facilities without moving deeply into the treatment area.

13. Computers are powered down during the evening hours.

14. The conference room is positioned away from the treatment rooms so that there is privacy between the clinical and business portions of the practice.

15. All counseling rooms are fitted with commercial sound deadening in the demising walls.

These conditions and procedures are reviewed on an annual basis during the last month of the year.

Chapter 13: Monitoring Compliance Procedures and Logs

On a quarterly basis our security officers review the logs kept in our clinic to assure that they are being used properly and kept up-to-date. They will also look for a potential for information leakage and will inspect the logs to make sure that they are being used on a regular basis and with every patients whose PHI has been accessed in any way.

Chapter 14: Contingency Plan

We have a contingency plan in place in the event there is a major disaster and it affects our facility. All electronic data is stored as backup storage that is cloud-based which will allow us to access information such as patient appointments and other patient information should our facility become inoperable for any reason. We will be able to meet with emergency patients in the event that our facility is not able to be occupied.

Chapter 15: Employees Access to Policies and Procedures

The information contained in this policy and procedure manual as well as our employee handbook and any other information that is been created electronically

and used for compliance, will be reduced to hard copy and made available to the staff. It can be found in the reception area closet cabinets in the conference room in a three ring binder entitled HIPAA Compliance Manual.

Conclusion

Providing security and privacy for PHI and for the protection of other patient information is an ongoing procedure which involves constant surveillance an update. We will update our major procedures once a year in December with other procedures such as logs and assessments done on a quarterly basis. We will also conduct assessments anytime there is a perceived or real breach of information security. The need for clinic compliance is evident and we will make every effort to conduct our business in a way that provides for compliance and patient protection.

Appendix

A: Acknowledgement of Receipt of Notice of Privacy Practices

B: Notice of Privacy Practices

C: Consent for Release of Medical Information

D: Security Incident Report

Peace of Mind Counseling

ACKNOWLEDGMENT OF RECEIPT OF NOTICE OF PRIVACY PRACTICES

Notice to Patient:

We are required to provide you with a copy of our Notice of Privacy Practices. The notice states how we may use and/or disclose your health information.

Please sign this form to acknowledge receipt of the Notice.

You may refuse to sign this acknowledgment, if you wish.

I acknowledge that I have received a copy of this office's Notice of Privacy Practices.

_____

Please print your name here

_____

Signature

_____

Date

FOR OFFICE USE ONLY

We have made every effort to obtain written acknowledgment of receipt of our Notice of Privacy from this patient, but it could not be obtained because:

□ The patient refused to sign.

□ Due to an emergency situation, it was not possible to obtain an acknowledgment.

□ We weren't able to communicate with the patient.

□ Other (please provide specific details) _____

_____ _____

Employee Signature Date

NOTICE OF PRIVACY PRACTICES

Peace of Mind Counseling

Privacy Officers, Ron Haynes & Otis Whigham 434.363.4815

Effective Date: November 3, 2014

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY. ANY REFERENCES IN THIS DOCUMENT TO MEDICAL PRACTICE, MEDICAL RECORDS, MEDICAL SERVICES, ETC. APPLY ALSO TO PSYCHOTHERAPY.

We understand the importance of privacy and are committed to maintaining the confidentiality of your medical information. We make a record of the medical care we provide and may receive such records from others. We use these records to provide or enable other health care providers to provide quality medical care, to obtain payment for services provided to you as allowed by your health plan and to enable us to meet our professional and legal obligations to operate this medical practice properly. We are required by law to maintain the privacy of protected health information, to provide individuals with notice of our legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information. This notice describes how we may use and disclose your medical information. It also describes your rights and our legal obligations with respect to your medical information. If you have any questions about this Notice, please contact our Privacy Officers listed above.

TABLE OF CONTENTS

A. How This Medical Practice May Use or Disclose Your Health Information

This medical practice collects health information about you and stores it in a chart [and on a computer][and in an electronic health record/personal health record]. This is your medical record. The medical record is the property of this medical practice, but the information in the medical record belongs to you. The law permits us to use or disclose your health information for the following purposes:

1. Treatment. We use medical information about you to provide your medical care. We disclose medical information to our employees and others who are involved in providing the care you need. For example, we may share your medical information with other physicians or other health care providers who will provide services that we do not provide. Or we may share this information with a pharmacist who needs it to dispense a prescription to you, or a laboratory that performs a test. We may also disclose medical information to members of your family or others who can help you when you are sick or injured, or after you die.

2. Payment. We use and disclose medical information about you to obtain payment for the services we provide. We may also disclose information to other health care providers to assist them in obtaining payment for services they have provided to you.

3. Health Care Operations. We may use and disclose medical information about you to operate this medical practice. For example, we may use and disclose this information to review and improve the quality of care we provide, or the competence and qualifications of our professional staff. Or we may use and disclose this information to get your health plan to authorize services or referrals. We may also use and disclose this information as necessary for medical reviews, legal services and audits, including fraud and abuse detection and compliance programs and business planning and management. We may also share your medical information with our "business associates," such as our billing service, that perform administrative services for us. We have a written contract with each of these business associates that contains terms requiring them and their subcontractors to protect the confidentiality and security of your protected health information. We may also share your information with other health care providers, health care clearinghouses or health plans that have a relationship with you, when they request this information to help them with their quality assessment and improvement activities, their patient-safety activities, their population-based efforts to improve health or reduce health care costs, their protocol development, case management or care-coordination activities, their review of competence, qualifications and performance of health care professionals, their training programs, their accreditation, certification or licensing activities, or their health care fraud and abuse detection and compliance efforts

4. Appointment Reminders. We may use and disclose medical information to contact and remind you about appointments. If you are not home, we may leave this information on your answering machine or in a message left with the person answering the phone.

5. Sign In Sheet. We may use and disclose medical information about you by having you sign in when you arrive at our office. We may also call out your name when we are ready to see you.

6. Notification and Communication With Family. We may disclose your health information to notify or assist in notifying a family member, your personal representative or another person responsible for your care about your location, your general condition or, unless you had instructed us otherwise, in the event of your death. In the event of a disaster, we may disclose information to a relief organization so that they may coordinate these notification efforts. We may also disclose information to someone who is involved with your care or helps pay for your care. If you are able and available to agree or object, we will give you the opportunity to object prior to making these disclosures, although we may disclose this information in a disaster even over your objection if we believe it is necessary to respond to the emergency circumstances. If you are unable or unavailable to agree or object, our health professionals will use their best judgment in communication with your family and others.

7. Marketing. Provided we do not receive any payment for making these communications, we may contact you to give you information about products or services related to your treatment, case management or care coordination, or to direct or recommend other treatments, therapies, health care providers or settings of care that may be of interest to you. We may similarly describe products or services provided by this practice and tell you which health plans this practice participates in. We may also encourage you to maintain a healthy lifestyle and get recommended tests, participate in a disease management program, provide you with small gifts, tell you about government sponsored health programs or encourage you to purchase a product or service when we see

you, for which we may be paid. Finally, we may receive compensation which covers our cost of reminding you to take and refill your medication, or otherwise communicate about a drug or biologic that is currently prescribed for you. We will not otherwise use or disclose your medical information for marketing purposes or accept any payment for other marketing communications without your prior written authorization. The authorization will disclose whether we receive any compensation for any marketing activity you authorize, and we will stop any future marketing activity to the extent you revoke that authorization.

8. Sale of Health Information. We will not sell your health information without your prior written authorization. The authorization will disclose that we will receive compensation for your health information if you authorize us to sell it, and we will stop any future sales of your information to the extent that you revoke that authorization.

9. Required by Law. As required by law, we will use and disclose your health information, but we will limit our use or disclosure to the relevant requirements of the law. When the law requires us to report abuse, neglect or domestic violence, or respond to judicial or administrative proceedings, or to law enforcement officials, we will further comply with the requirement set forth below concerning those activities.

10. Public Health. We may, and are sometimes required by law, to disclose your health information to public health authorities for purposes related to: preventing or controlling disease, injury or disability; reporting child, elder or dependent adult abuse or neglect; reporting domestic violence; reporting to the Food and Drug Administration problems with products and reactions to medications; and reporting disease or infection exposure. When we report suspected elder or dependent adult abuse or domestic violence, we will inform you or your personal representative promptly unless in our best professional judgment, we believe the notification would place you at risk of serious harm or would require informing a personal representative we believe is responsible for the abuse or harm.

11. Health Oversight Activities. We may, and are sometimes required by law, to disclose your health information to health oversight agencies during the course of audits, investigations, inspections, licensure and other proceedings, subject to the limitations imposed by law.

12. Judicial and Administrative Proceedings. We may, and are sometimes required by law, to disclose your health information in the course of any administrative or judicial proceeding to the extent expressly authorized by a court or administrative order. We may also disclose information about you in response to a subpoena, discovery request or other lawful process if reasonable efforts have been made to notify you of the request and you have not objected, or if your objections have been resolved by a court or administrative order.

13. Law Enforcement. We may, and are sometimes required by law, to disclose your health information to a law enforcement official for purposes such as identifying or locating a suspect, fugitive, material witness or missing person, complying with a court order, warrant, grand jury subpoena and other law enforcement purposes.

14. Coroners. We may, and are often required by law, to disclose your health information to coroners in connection with their investigations of deaths.

15. Public Safety. We may, and are sometimes required by law, to disclose your health information to appropriate persons in order to prevent or lessen a serious and imminent threat to the health or safety of a particular person or the general public.

16. Specialized Government Functions. We may disclose your health information for military or national security purposes or to correctional institutions or law enforcement officers that have you in their lawful custody.

17. Workers' Compensation. We may disclose your health information as necessary to comply with workers' compensation laws. For example, to the extent your care is covered by workers' compensation, we will make periodic reports to your employer about your condition. We are also required by law to report cases of occupational injury or occupational illness to the employer or workers' compensation insurer.

18. Change of Ownership. In the event that this medical practice is sold or merged with another organization, your health information/record will become the property of the new owner, although you will maintain the right to request that copies of your health information be transferred to another physician or medical group.

19. Breach Notification. In the case of a breach of unsecured protected health information, we will notify you as required by law. If you have provided us with a current e-mail address, we may use e-mail to communicate information related to the breach. In some circumstances our business associate may provide the notification. We may also provide notification by other methods as appropriate. [Note: Only use e-mail notification if you are certain it will not contain PHI and it will not disclose inappropriate information. For example if your e-mail address is "digestivediseaseassociates.com" an e-mail sent with this address could, if intercepted, identify the patient and their condition.]

20. Psychotherapy Notes. We will not use or disclose your psychotherapy notes without your prior written authorization except for the following: 1) use by the originator of the notes for your treatment, 2) for training our staff, students and other trainees, 3) to defend ourselves if you sue us or bring some other legal proceeding, 4) if the law requires us to disclose the information to you or the Secretary of HHS or for some other reason, 5) in response to health oversight activities concerning your psychotherapist, 6) to avert a serious and imminent threat to health or safety, or 7) to the coroner or medical examiner after you die. To the extent you revoke an authorization to use or disclose your psychotherapy notes, we will stop using or disclosing these notes.

21. Research. We may disclose your health information to researchers conducting research with respect to which your written authorization is not required as approved by an Institutional Review Board or privacy board, in compliance with governing law.

22. Fundraising. We may use or disclose your demographic information in order to contact you for our fundraising activities. For example, we may use the dates that you received treatment, the department of service, your treating physician, outcome information and health insurance status to identify individuals that may be interested in participating in fundraising activities. If you do not want to receive these materials, notify the Privacy Officers listed at the top of this Notice of Privacy Practices and we will stop any further fundraising communications. Similarly, you should notify the Privacy Officers if you decide you want to start receiving these solicitations again.

B. When This Medical Practice May Not Use or Disclose Your Health Information

Except as described in this Notice of Privacy Practices, this medical practice will, consistent with its legal obligations, not use or disclose health information which identifies you without your written authorization. If you do authorize this medical practice to use or disclose your health information for another purpose, you may revoke your authorization in writing at any time.

C. Your Health Information Rights

1. Right to Request Special Privacy Protections. You have the right to request restrictions on certain uses and disclosures of your health information by a written request specifying what information you want to limit, and what limitations on our use or disclosure of that information you wish to have imposed. If you tell us not to disclose information to your commercial health plan concerning health care items or services for which you paid for in full out-of-pocket, we will abide by your request, unless we must disclose the information for treatment or legal reasons. We reserve the right to accept or reject any other request, and will notify you of our decision.

2. Right to Request Confidential Communications. You have the right to request that you receive your health information in a specific way or at a specific location. For example, you may ask that we send information to a particular e-mail account or to your work address. We will comply with all reasonable requests submitted in writing which specify how or where you wish to receive these communications.

3. Right to Inspect and Copy. You have the right to inspect and copy your health information, with limited exceptions. To access your medical information, you must submit a written request detailing what information you want access to, whether you want to inspect it or get a copy of it, and if you want a copy, your preferred form and format. We will provide copies in your requested form and format if it is readily producible, or we will provide you with an alternative format you find acceptable, or if we can't agree and we maintain the record in an electronic format, your choice of a readable electronic or hardcopy format. We will also send a copy to any other person you designate in writing. We will charge a reasonable fee which covers our costs for labor, supplies, postage, and if requested and agreed to in advance, the cost of preparing an explanation or summary. We may deny your request under limited circumstances. If we deny your request to access your child's records

or the records of an incapacitated adult you are representing because we believe allowing access would be reasonably likely to cause substantial harm to the patient, you will have a right to appeal our decision. If we deny your request to access your psychotherapy notes, you will have the right to have them transferred to another mental health professional.

4. Right to Amend or Supplement. You have a right to request that we amend your health information that you believe is incorrect or incomplete. You must make a request to amend in writing, and include the reasons you believe the information is inaccurate or incomplete. We are not required to change your health information, and will provide you with information about this medical practice's denial and how you can disagree with the denial. We may deny your request if we do not have the information, if we did not create the information (unless the person or entity that created the information is no longer available to make the amendment), if you would not be permitted to inspect or copy the information at issue, or if the information is accurate and complete as is. If we deny your request, you may submit a written statement of your disagreement with that decision, and we may, in turn, prepare a written rebuttal. All information related to any request to amend will be maintained and disclosed in conjunction with any subsequent disclosure of the disputed information.

5. Right to an Accounting of Disclosures. You have a right to receive an accounting of disclosures of your health information made by this medical practice, except that this medical practice does not have to account for the disclosures provided to you or pursuant to your written authorization, or as described in paragraphs 1 (treatment), 2 (payment), 3 (health care operations), 6 (notification and communication with family) and 18 (specialized government functions) of Section A of this Notice of Privacy Practices or disclosures for purposes of research or public health which exclude direct patient identifiers, or which are incident to a use or disclosure otherwise permitted or authorized by law, or the disclosures to a health oversight agency or law enforcement official to the extent this medical practice has received notice from that agency or official that providing this accounting would be reasonably likely to impede their activities.

6. Right to a Paper or Electronic Copy of this Notice. You have a right to notice of our legal duties and privacy practices with respect to your health information, including a right to a paper copy of this Notice of Privacy Practices, even if you have previously requested its receipt by e-mail.

If you would like to have a more detailed explanation of these rights or if you would like to exercise one or more of these rights, contact our Privacy Officers listed at the top of this Notice of Privacy Practices.

D. Changes to this Notice of Privacy Practices

We reserve the right to amend this Notice of Privacy Practices at any time in the future. Until such amendment is made, we are required by law to comply with the terms of this Notice currently in effect. After an amendment is made, the revised Notice of Privacy Protections will apply to all protected health information that we maintain, regardless of when it was created or received. We will keep a copy of the current notice posted in our reception area, and a copy will be available at each appointment. We will also post the current notice on our website.

E. Complaints

Complaints about this Notice of Privacy Practices or how this medical practice handles your health information should be directed to our Privacy Officers listed at the top of this Notice of Privacy Practices.

If you are not satisfied with the manner in which this office handles a complaint, you may submit a formal complaint by using the form from the website below:

The complaint form may be found at **www.hhs.gov/ocr/privacy/hipaa/complaints/hipcomplaint.pdf**. You will not be penalized in any way for filing a complaint

Peace of Mind Counseling

Security Incident Report

Date: _____

Description of Security Incident:

_____
_____
_____
_____
_____
_____

Measures Taken to Resolve the Problem or Mitigate Effects:

_____
_____
_____
_____
_____
_____

Steps Taken to Prevent Recurrence:

_____
_____
_____
_____
_____
_____

Security Officer: _____

_____

Signature of Security Officer

Authorization for the Release of Healthcare Records

Patient Name:_____ Date of Birth:_____
(also list maiden name/other names used)

I hereby request and authorize: **_____ of Peace of Mind Counseling**

3311 Old Forest Rd, Ste. 101

Lynchburg, VA 24501

____To Disclose info ____To Receive Info or ____To Exchange Information with

Provider:_____

Address:_____

City/State/Zip_____

Information to be disclosed includes copies of:

_____Entire Record _____Progress Notes

_____Other: _____

This authorization will be effective for one year after the date signed, unless cancelled in writing. I understand that the cancellation will have no effect on information released prior to receiving the cancellation. A copy of this authorization is as valid as the original.

_____Date:_____
Signature of Patient

If signing for a minor patient, I hereby state that my parental rights have not been revoked by a court of law.

_____/_____Date:_____
Signature of Legal Representative/Relationship

Notice to recipient of information: This information has been disclosed to you from confidential records, which are protected by law. Unless you have further authorization, laws may prohibit you from making any further disclosures of this information without the specific written consent of the patient or legal representative.

Compliance Forms and Logs

Compliance Forms and Logs

Employee Non-disclosure Agreement

Employee Breach From

Privacy Officer Agreement

HIPAA Training Log

Personnel Clearance Type

Compliance Procedure Quiz

List of Devices Inventory

Work Station Inventory

Identification of Persons with Authorization to Access PHI

Employee Agreement

Violation Form

Annual Review of Privacy Procedures (chapter 12)

Compliance Officer Training

Monitoring Compliance Procedure and Logs

Restriction of PHI Disclosure

Risk Assessment Form

Employee Non-disclosure Agreement

The Agreement is entered into this day between Peace of Mind Counseling and _____ (Hereafter known as “Employee”).

The above agree to the following:

EMPLOYEE shall not:

1. Disclose any patient information to any party outside the office. This will include patient names, addresses, phone numbers conditions and all other private patient information.
2. Discuss any patient’s information or conditions with anyone outside the employment of the office.
3. Discuss any part of the patient's information or conditions with other employees except as necessary to conduct normal business.
4. Release any information in any electronic or tangible form including patient information by word processing, fax, e-mail, video transmission or other means.
5. Divulge any passwords or usernames or other information which would assist someone in accessing PHI.
6. Allow data to remain on the computer screen or other device that can be readily seen by others.
7. Withhold information regarding potential violation of patient privacy and shall report any potential privacy breach to the privacy officer of this facility.

I agree to the above.

_____ _____

Signature of Employee Date

Employee Breach Form

Employees Name _____ Date _____

Explanation of Violation:

_____

_____

_____

_____

_____

Date of Violation: _____

Action to Be Taken:

[ ] Training

[ ] Warning

[ ] Probation

[ ] Termination

[ ] Other _____

I have read and understand the information contained in this notice.

Date: _____

_____ _____

Employee Signature HIPAA Officer Signature

Privacy Officers Agreement

Date _____

As of the above date Ron Haynes & Otis Whigham will function as both security and privacy officers. Staff will be informed of their role as privacy officers. Their duties will include:

1. Manage the implementation of any and all omnibus rules program

2. Report to management on a regular basis regarding the implementation of compliance procedures

3. Create and maintain a compliance training program for employees

4. Provide agreements for business associates and maintain their files

5. Act on matters of potential noncompliance

6. Report all breaches of more than a low probability

7. Place a written document explaining each breach in the back of this manual

8. Take corrective action with all employees

9. Develop new programs and policies to help protect PHI

If the privacy officers need outside help to conduct a security risk assessment they have the power to employ a nonbiased party to assist in assessment.

They are responsible for knowing HIPAA regulations, training clinic staff in HIPAA compliance, and assuring that HIPAA-related policies and procedures are instituted and followed. They will:

1. Update HIPAA policies and procedures and place them in this manual.

2. Oversee the implementation of the policies and procedures contained in this Manual.

3. Ensure that all clinic personnel are trained according to HIPAA and the policies and procedures of the clinic.

4. Review activity that takes place in the clinic to detect security risks.

5. Investigate and respond to potential security breaches and take appropriate action in the event of a breach in security, and eliminate or mitigate any damaging effects.

As privacy managers, we agree to perform the above duties.

_____ _____

Signature Date

_____ _____

Signature Date

HIPAA Training Log

I have received the HIPAA training or re-training and have passed the Training test as of the date shown below.

Name	Signature	Training Date
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Personnel Clearance Type

Name	Signature	Type 1-5
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Compliance Procedure Quiz

Name_____ Date _____

True of False

_____ 1. Peace of Mind Counseling is a covered entity and must abide by all HIPAA rules and regulations.

_____ 2. Each new patient must sign an Acknowledgement of Receipt of Privacy Practice Policy form on the first visit.

_____ 3. Peace of Mind Counseling must provide patients with a copy of the Privacy Practice Policy form on the first visit.

_____ 4. It is best to use just the patient's first name if they must be addressed in the reception room or any public area in the clinic.

_____ 5. Releasing patient's names, as long as no phone number is released, is not a HIPAA violation.

_____ 6. All suspected violations should be reported to our to our compliance officer.

_____ 7. All patients' records must be stored in a locked place after hours.

_____ 8. We can contact the patient's by g-mail as long as we have their permission.

_____ 9. We can text appointment times to our patients by cell phone.

_____ 10. We must have a "Release of Medical Information" Form signed before we can release patient's information.

11. _____are our compliance officers.

12. Our clinic's compliance manual is located _____.

List of Devices Inventory

Name of Device _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Device _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Device _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Device _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Device _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Device _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

_____

Name of Device _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Device _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Device _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Work Station Inventory

Name of Work Station _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Work Station _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Work Station _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Work Station Inventory

Name of Work Station _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Work Station _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Work Station _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Work Station Inventory

Name of Work Station _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Work Station _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Work Station _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Work Station Inventory

Name of Work Station _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Work Station _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Work Station _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Work Station Inventory

Name of Work Station _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Work Station _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Name of Work Station _____

Location _____

Use _____

Date Taken Out of Service _____

Method of Disposal _____

_____

Identification of Persons with Authorization to Access Patient Health Information

Those individuals or parties that could have access to Patient Health Information at Peace of Mind Counseling include but may not be limited to:

The staff of Breakthrough Counseling. This includes:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____

Necessary health care providers or vendors who may need to be consulted if related to the patient's condition. This includes:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

I verify that this information concerning who has access to PHI and what types of PHI is requested in this office is accurate and current:

Owner Name Signature Date

Owner Name Signature Date

Employee Agreement

Date: _____

Peace of Mind Counseling office is an organization whose mission is to provide the most cost effective counseling while maintaining high quality and integrity. The clinic also strives to be fully compliant with all of the complex rules and regulations governing the healthcare industry. As a result, the clinic has launched this compliance program.

It is the office's desire for this program to aid in the identification and correction of any actual or perceived violations of any applicable HIPAA regulations and clinic policy. In order to achieve this goal, this compliance program imposes a duty upon all employees to report to designated individuals any actual or perceived violation occurring in the office.

Ron Haynes & Otis Whigham are the office's compliance officers. It is the office's expectation that each employee should feel free to communicate his or her concerns to one of the Compliance Officers. The office will treat any such report confidentially and consistently with fair and rigorous enforcement of the compliance program. It is the office's express policy that no adverse action or retribution will be taken by the office against any employee due to an employee's good faith reporting of a suspected violation or irregularity.

All employees should familiarize themselves with the HIPAA Compliance Program. The therapist or the Privacy Official is available to answer any questions you may have.

The Peace of Mind Counseling office is committed to conducting its business lawfully and ethically. As the clinic's reputation is the sum of the reputation of its employees, it is critically important that all of its employees meet the highest standards of legal and ethical conduct. Any doubts whatsoever as to the appropriateness of a particular situation should be submitted either to one of the Privacy Officers. Any employee violating any provision of this Compliance Program will be subject to disciplinary action, up to and including discharge from employment.

All employees must comply scrupulously with all federal, state, and local laws and government regulations and immediately report any discrepancies or inactions to a Compliance Officer. This should include any actual or perceived violations.

I have read, I understand and agree to abide by the above information.

_____ _____

Employee Signature Date

VIOLATION FORM

Date:	Number:
Compliance Officer:	
Person/Party Alleging Violation:	
Address:	
Day Time Phone:	Evening Phone:
Does the Party want to remain anonymous? ☐ Yes ☐ No	

Description of Alleged Violation: _____

_____

_____

_____

_____

_____

_____

VIOLATION REVIEW

The above alleged violation was investigated using: (check all that apply)

☐ Personal interview of therapist

☐ Personal interview of staff

☐ Personal interview of patients

☐ Personal interview of third party payer

☐ Records and/or billing review

☐ Additional written information/documentation is attached

After reviewing the activity reported above

☐ was ☐ was not a violation of Federal, State or other laws, regulations or other directives.

Reason:

_____

_____

_____	_____	_____	_____
Therapist's Signature	Date	Compliance Officer's Signature	Date

Actions Taken

1. Termination of Activities: _____

_____

_____

2. Penalties Assessed: _____

_____

_____

3. Training: _____

_____

_____

4. Discipline: _____

_____

_____

5. Review: _____

_____

_____

Comments: _____

_____

_____

_____

Therapists Signature	Date	Compliance Officer's Signature	Date
_____	_____	_____	_____

Annual Review of Privacy Procedures

Any questions answered in the negative should be addressed in the comment section below.

Physical Facility

1. Do we provide white noise in the reception area to dampen transmission of sound?

2. Are patient files and other private records filed away so they are not seen on the front desk or other public areas?

3. Are the workstations in the reception area facing away from patient traffic?

4. Is the door between the reception area and the clinical area kept closed and locked during nonclinical hours?

5. Is music or other white noise playing outside the individual therapy offices?

6. Are the doors to the counseling rooms closed during therapy sessions?

7. Are the workstations in the counseling rooms facing away from patient flow and/or are they using adequate screensavers?

8. Are file cabinets containing patient records locked at night?

9. Is the computer system backed up on a regular basis?

Office Procedure

1. Does the patient sign the acknowledgment of receipt of privacy practice policies during the first visit?

2. Do new patients receive a copy of the privacy practice policies during the first visit?

3. Are patients addressed only by the first name whenever possible?

4. Are workstations and counseling rooms kept free of patient files that are not in use?

5. Are patient files stored back to the proper position immediately after use?

6. Is clinical and administrative staff receiving compliance training within 30 days of employment?

7. Is clinical and administrative staff receiving continuing training on an annual basis?

8. Have the clinical and administrative staff pass the appropriate training quiz?

9. Are computer passwords being changed on a regular basis?

10. Are computer passwords sufficiently difficult to prevent interception?

11. Are all potential violations reported to the compliance officers?

12. Are all potential violations being adequately investigated?

13. Are all violations being corrected?

14. Are patient records being kept with electronic health records?

15. Has proper procedure been followed after the voluntary or involuntary termination of employees?

16. Are business associate agreements being signed by those who qualify as a business associate?

17. Is the compliance manual being kept in a place that is available to all employees?

18. Are the employees aware of the location of the compliance manual?

19. Has the clinic updated or introduced any new forms necessary for compliance?

20. Has the HIPAA retraining and updating of the compliance manual been done during the month of December as our policies call for?

Are there any changes that need to be made to the physical facility, office procedure or compliance procedures? Please comment below.

_____
_____
_____
_____
_____
_____
_____
_____

Compliance Officers Log

I agree to function as the clinic’s Compliance Officer witnessed by my signature below.

Name (print)	Name (signature)	Date Started	Date Ended

Monitoring Compliance Procedure and Logs

Quarterly Reviews

Date of Review _____

Findings:

_____
_____
_____
_____
_____
_____
_____

Date of Review _____

Findings:

_____
_____
_____
_____
_____
_____

Date of Review _____

Findings:

_____
_____
_____
_____
_____
_____
_____

Date of Review _____

Findings:

_____
_____
_____
_____
_____
_____
_____

Date of Review _____

Findings:

_____
_____
_____
_____
_____
_____

Date of Review _____

Findings:

_____
_____
_____
_____
_____
_____
_____

Date of Review _____

Findings:

_____
_____
_____
_____
_____
_____
_____

Date of Review _____

Findings:

_____
_____
_____
_____
_____
_____

Date of Review _____

Findings:

_____
_____
_____
_____
_____
_____
_____

Date of Review _____

Findings:

_____
_____
_____
_____
_____
_____
_____

Date of Review _____

Findings:

_____
_____
_____
_____
_____
_____

Date of Review _____

Findings:

_____
_____
_____
_____
_____
_____
_____

Restriction of PHI Disclosure

Name of Patient: _____

Date of Request: _____

Type of Restriction Requested:

_____
_____
_____
_____
_____

By signing below, Peace of Mind Counseling agrees to restrict release of patient's health information as described above. Certain restrictions cannot be honored such as disclosures required by law, disclosures related to crimes in the facility, or disclosures necessary to avoid serious threat of safety in emergencies.

This restriction may be only be terminated by written consent of the patient or legal guardian.

I request the restrictions listed above.

_____ _____

Patient's Signature Date

THERAPIST APPROVAL

I agree to restrict the disclosure of personal health information as requested above.

_____ _____

Therapist Signature Date

Risk Assessment Form

1. Was PHI released? _____

2. Was the PHI of highly sensitive nature? *If any of the below PHI was released the incident should be reported.*

a. Patient's full name with address

b. Patient's full name with telephone number

C. Patient's full name with Social Security number

D. Patient's full name and test results

E. Patient's full name and license number

F. Patient's full name and fingerprint

G. Patient's full name and credit card number

H. Patient's full name and vehicle ID

I. Patient's full name and web address

J. Patient's full name and diagnosis

K. Patient's full name and any sensitive medical information

3. Is medical information likely to be linked to the patient? _____

4. Was the PHI of low sensitivity? _____

A. Partial patient name

B. Patient name without any medical records or personal information attached

C. Patient's name or other identifying factor with general medical information only such as name of hospital.

5. Was the recipient high or low risk?_____ Entities like other health facilities, insurance carriers, pharmacies or our patients are low risk. Entities like people or

businesses who are unknown, stolen information, hacked into information and unknown recipients are high risk.

6. Was PHI actually acquired and reviewed? _____

7. Can PHI be located in suppressed? Can the information be located by a phone call, e-mail letter or text with instructions to destroy it? _____

High sensitivity breaches should be reported. Low sensitivity breaches do not need to be reported.

Breaches should be reported to:

Secretary of the US Department of Health and Human Services at:

http://hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/instruction.html

The breach [ ] was [ ] was not reported for the following reason(s).

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____ _____
Signature of Security Officer Date

_____ _____
Signature of Security Officer Date