Table of Contents
HIPAA Policies and Procedures

The policies, procedures and forms of Practice shall be periodically reviewed and updated consistent with the requirements and standards established by the Board of Directors and by Practice management, federal and state law and regulations, and applicable accrediting and review organizations.

POLICIES

FORMS

Administrative Forms

A-1 Notice of Privacy Practices (separate file)

Patient Rights Forms

F-1: Request to Copy and Inspect
F-2: Request Amendment to Health Information
F-3: List of Non Routine Disclosures
F-4: Patient Complaint Form

Workforce Forms

F-5: Confidentiality Agreement
F-6: Training Log
F-7: Privacy Testing Tool

Disclosure Forms

F-8: Authorization for Non Routine Disclosures

Practice **POLICY & PROCEDURE** **MANUAL:** Administrative **SECTION:** HIPAA Administrative **SUBJECT:** Handing of Privacy Complaints	Policy # HIPAA A-1 Total Pages: 2 Effective Date: Approved:

PURPOSE: The purpose of this policy is to comply with the requirements of the Privacy Rule and to afford patients the right to file a complaint, have the complaint investigated, and, if appropriate, understand how Practice has addressed the complaint.

POLICY: It is Practice's policy to keep a record of all complaints and to investigate all complaints to determine the circumstances surrounding any concerns that patients raise regarding privacy. If there is evidence that a member of Practice's workforce or business associate has not adhered to Practice policy and procedure or a standard, specification or other requirement of the Privacy Rule, Practice will take actions consistent with the Privacy Rule and its policies and procedures, including its policies and procedures on sanctions and mitigation of harm, and document these actions accordingly.

Under no circumstances will the fact that a patient has filed a complaint affect the services provided to that patient, and any retaliation shall be subject to sanction by Practice.

PROCEDURE:

Patients who wish to file a privacy complaint will be provided with a Complaint Form (###) and instructed to submit the form or letter to:

Privacy Officer
Practice
Address
Address
Address

Alternatively, patient may be instructed to call our Privacy Officer, or may register a verbal complaint directly to any member of the management team.

If a privacy complaint is filed by a patient, the employee receiving the complaint will forward the complaint to the Privacy Officer who will validate the complaint with the patient by contacting or meeting with the patient, and will confirm the patient's name and other identifying information, to validate the facts of the complaint.

The Privacy Officer will document all complaints in the privacy complaint log, and will investigate the complaint. If the process of investigation reveals that the conduct of Practice personnel was appropriate, patient will be notified as such, and the documentation of the investigation will be maintained by Practice. If it is determined that the complaint is valid, the Privacy Officer, will develop an appropriate response, which may include disciplinary action, and / or appropriate action to mitigate the harmful effects of the privacy violation. Practice will draft a letter explaining the findings of its investigation and actions in response to the complaint. The Privacy Officer will document the disposition of the complaint on the privacy complaint log and file the letter in the “investigated privacy complaints” file.

The Privacy Officer will review its privacy complaint file periodically and attempt to use the experience to improve workforce training related to the violation.

___Mendy Maccabee MD_____ _____

Privacy Officer Date 9/28/2019

Practice **POLICY & PROCEDURE** **MANUAL:** Administrative **SECTION:** HIPAA Administrative **SUBJECT:** Designated Record Set	Policy # HIPAA A-2 Total Pages: 2 Effective Date: Approved:

PURPOSE: The purpose of this policy is to comply with the Privacy Rule Standard that provides patients the right to obtain a copy of protected health information about them in a Designated Record Set.

POLICY: It is the policy of Practice to assist patients with access to individually identifiable health information (Protected Health Information) maintained by Practice

DEFINITION:
The Designated Record Set of Practice consists of:

- Financial Records:
  Patient demographics such as name, address, SSN, phone number, insurance information, employment information, and other information necessary to complete financial operations. Also explanations of benefits, claims, remittance reports, the patients financial history.

Medical Records:
Patient progress notes, diagnostic test reports, EKG reports, laboratory notebook, x-ray library file

The Designated Record Set excludes the following:

Original source documents such as X-ray films, Holter monitor tapes, Echo strips, pictures, and videos unless interpretations, summarizations, or transcriptions are not available
All other physical testing artifacts from which a report is derived, that will reside in the record set above
Documents pertaining to administrative compliance such as Quality Assurance data and Chart audit reports, or administrative procedures such as authorization for release of information forms, claim forms, lab requisitions, or data aggregation
De-identified information
Psychiatric Notes
Information compiled in advance of a civil, criminal, or administrative proceeding
Consultation reports and copies of records received from other health care providers
Information maintained by a Business Associate of Practice

PROCEDURE:

To be completed by practice - Answer the question – “where can this data be obtained”?

To be completed by practice - Answer the question –“where and when will the information be available”. Keep in mind that customer service is an important consideration.

_____ _____

Privacy Officer Date

Practice **POLICY & PROCEDURE** **MANUAL:** Administrative **SECTION:** HIPAA Administrative **SUBJECT:** Duty to Report and Mitigate	Policy # HIPAA A-3 Total Pages: 1 Effective Date: Approved:

PURPOSE: The purpose of this policy is to comply with the Privacy Rule Standard that requires covered entities to mitigate, to the extent possible, any known harmful effect due to a violation of its policies and procedures or requirements of the HIPAA regulations.

POLICY: It is the policy of Practice to report and / or to take immediate action to minimize the harmful effect of non compliance with our HIPAA policies and procedures. Our intent is to remedy any harm caused by the mistake, and to prevent the mistake from happening again. Nor will Practice condon any act of retaliation against a patient who files a complaint based or brings a possible violation to our attention.

PROCEDURE:

Suspected violations of the HIPAA regulations are to be reported to a member of the management team or the Privacy Officer immediately. Further, employees are expected to use professional judgment to take immediate action when warranted to:

Take action to discontinue the improper use or disclosure, and
Employ such means as are available to retrieve improperly disclosed health information.

Practice may apply appropriate sanctions, which may include, but are not limited to, reprimand, demotion, suspension and/or termination.

Practice will evaluate if additional policies, procedures or safeguards are required to minimize future risks of noncompliance, and will undertake appropriate training and education to prevent a recurrence of the improper use or disclosure.

Suspected violations involving a Business Associate will be investigated by the Privacy Officer, who will make a report and recommendation for action to the governing body of Practice.

_____ _____

Privacy Officer Date

Practice **POLICY & PROCEDURE** **MANUAL:** Administrative **SECTION:** HIPAA Administrative **SUBJECT:** Business Associate Agreement	Policy # HIPAA A-4 Total Pages: 1 Effective Date: Approved:

PURPOSE: The purpose of this policy is to extend the safeguards for use and disclosure of PHI to those entities that are independent of Practice and with whom we share PHI to conduct our business.

POLICY: It is the policy of Practice to identify and obtain a written Business Associate Agreement with entities and persons who have access to PHI.

DEFINTION:
A "business associate" is a person or entity who provides certain functions, activities, or services for or to Practice involving the use and/or disclosure of protected health information.

A person who is a member of Practice's workforce, i.e., an employee, volunteer, trainee and other person whose conduct is under the direct control of Practice, is not a business associate. A physician or other provider who receives protected health information for treatment purposes is also not a business associate.

PROCEDURE:
The Privacy Officer will create a Business Associate Agreement that will include a written understanding of Practice's expectations with regard to safeguarding the PHI of our patients, and will comply with the intent of the HIPAA Privacy Regulations.

Business associates who are providing functions, activities or services prior to April 14, 2003 will be required to enter into a formal agreement with (Your Practice) by _____ .

Business associate services commencing after April 14, 2003 will be required to enter into a formal written agreement prior to commencing work with Practice.

_____ _____
Privacy Officer Date

Practice **POLICY & PROCEDURE** **MANUAL:** Administrative **SECTION:** HIPAA Administrative **SUBJECT:** Privacy Officer Job Desc.	Policy # HIPAA A-5 Total Pages: 1 Effective Date: Approved:

PURPOSE: The purpose of this policy is to comply with the Privacy Rule Standard that requires covered entities to appoint a Privacy Officer who will have the responsibility for planning and implementing the HIPAA regulations.

POLICY: It is the policy of Practice to appoint and support the efforts of a Privacy Officer to lead Practice's HIPAA compliance efforts.

PROCEDURE:
Practice will approve and update as required a job description for a Privacy Officer. The Job Description is appended to this policy and will be filed in the HIPAA Manual.

_____ _____
Privacy Officer Date

Practice

PRIVACY OFFICER JOB RESPONSIBILITIES

The Privacy Officer for this practice oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the practice's policies and procedures related to the privacy of and access to patients' protected health information (PHI) in compliance with federal and state laws and the practice's privacy practices (the "Privacy Policy").
Responsibilities:

Maintain current knowledge of applicable federal and state privacy laws.

Develop, oversee and monitor implementation of the practice's Privacy Policy and ensure that the integrity of the Privacy Policy is maintained at all times.

Report regularly to the practice governing body and officers (as applicable) regarding the status of the Privacy Policy.

Work with legal counsel, management and committees to ensure that the practice maintains appropriate privacy consent and authorization forms, notices and other administrative materials in accordance with practice management and legal requirements.

Establish and administrate a process for receiving, documenting, tracking, investigating and taking action on all complaints concerning the practice's privacy policies and procedures in coordination and collaboration with other similar functions, and, when necessary, with legal counsel.

Establish and oversee practice policies for addressing patient requests to obtain or amend patient records, restrict the means of communication, or obtain accountings of disclosures; ensure compliance with practice policies and legal requirements regarding such requests and establish and oversee grievance and appeals processes for denials of requests related to patient access or amendments.

Oversee, direct, deliver, or ensure the delivery of privacy training and orientation to all employees, volunteers, medical and professional staff, and other appropriate personnel and maintain appropriate documentation of privacy training.

Monitor attendance at all Privacy Policy training sessions and evaluate participants' comprehension of the information provided at training sessions.

Monitor compliance with Privacy Policy including periodic privacy risk assessments.

Monitor and evaluate, on no less than an annual basis, the Privacy Policy's success in meeting the practice's goal for protection of PHI.

Coordinate and participate in disciplinary actions related to the failure of practice workforce members to comply with the practice Privacy Policy and/or applicable law.

Monitor technological advancements related to protected health information protection and privacy for consideration of adaptation by the practice.

Coordinate and facilitate the allocation of appropriate resources for the support of and the effective implementation of the Privacy Policy.

Initiate, facilitate and promote activities to foster privacy information awareness within the practice.

Cooperate with the Office of Civil Rights, other legal entities, and practice officers in any compliance reviews or investigations.

Perform periodic risk assessments and ongoing compliance monitoring activities at each practice location.

Act as point of contact for practice legal counsel in an ongoing manner and in the event of a reported violation.

Maintain all business associate contracts and respond appropriately if problems arise.

Act as the practice-based point of contact for receiving, documenting and tracking all complaints concerning privacy policies and procedures of the practice.

Skills:

Able to facilitate change.
Possess knowledge and understanding of privacy regulations and office technology

Practice **POLICY & PROCEDURE** **MANUAL:** Administrative **SECTION:** HIPAA Administrative **SUBJECT:** Notice of Privacy Practices	Policy # HIPAA A-6 Total Pages: 1 Effective Date: Approved:

PURPOSE: The purpose of this policy is to comply with the HIPAA Privacy Rule standards related to providing a Notice of Privacy Practices.

POLICY: Practice will make a reasonable effort to make its Notice of Privacy Practices available to its patients, and to comply with the commitments contained therein.

PROCEDURE:
Practice will post one or more Notices of Privacy Practices in prominent location(s). The Notice will include the provisions and requirements set forth in the regulations.

Copies of the Notice will be available at the front desk and our reception staff will encourage patients to take a copy as part of the check-in or check-out process for each visit. The emphasis will continue through 2003 and thereafter the Notices will be available upon request. [NOTE – IF YOU INTEND TO BE MORE AGGRESSIVE WITH CAPTURING SIGNATURES, INDICATE YOUR PLAN HERE]

Subsequent to reviewing the Notice, patients who have questions will be referred to the Privacy Officer or Practice Administrator.

The Notice of Privacy Practices will be provided to all new patients of the practices, and each will be asked to sign the acknowledgment that they have reviewed the Notice and had the opportunity to ask questions regarding Practice privacy practices.

Practice will promptly revise and distribute its Notice and, as applicable, will revise its written policies and procedures, whenever there is a material change to the uses or disclosures, patient rights, or other privacy practice stated in the Notice.

_____ _____
Privacy Officer Date

Practice **POLICY & PROCEDURE** **MANUAL:** Administrative **SECTION:** HIPAA Patient Rights **SUBJECT:** Right to Inspect and Copy	Policy # HIPAA P-1 Total Pages: 3 Effective Date: Approved:

PURPOSE: To provide guidelines to comply with the HIPAA privacy regulation's requirement to allow patients to access their protected health information

POLICY: It is Practice policy to provide patients the right to inspect and obtain a copy of their protected health information.

PROCEDURE:

A patient may access protected health information in a designated record set for as long as the information is maintained in the designated record set.

Practice will act on a patient's request for access within 30 days of receiving the request. If the information is not maintained or accessible on-site, Practice will act on a patient's request for access within 60 days of receiving the request. If Practice is unable to act on a request within the time period required, we may extend the timeframe by no more than 30 days by providing the patient with a written statement outlining the reasons for the delay and the date by which action on the request will be completed.

Practice will provide the patient with access to the protected health information in the form or format requested by the patient. If the information is not readily producible in such a form or format, the practice must provide the information in readable hard copy.

Practice may provide the patient with a summary of the health information requested or an explanation of the health information if the patient agrees to in advance to such a summary or explanation. Practice will charge a fee of $50 for providing a summary or explanation if the patient agrees in advance to such a fee.

If the patient requests a copy of the health information or agrees to a summary or explanation, Practice will charge a reasonable cost-based fee of $10, plus 5 cents per page to offset the cost of copying (including the cost of supplies and labor) and postage.

Practice may deny a patient access to health information without permitting the patient to request a review of the practice's decision not to provide access in the following circumstances:

- The information contains psychotherapy notes;

- The information was complied in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding;

- The information is subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the patient would be prohibited by law or exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2);

- The request is from an inmate of a correctional institution, and Practice believes that providing a copy of the health information would jeopardize the health, safety, security, custody or rehabilitation of the patient or other inmates, or would threaten the safety of any officer, employee or other person at the correctional institution;

- The patient has agreed to the denial of access when consenting to participate in a research study that includes treatment;

- The patient's access to the health information is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a if the denial of access under the Privacy Act would meet the requirements of that law; and

- The health information was obtained from someone other than a health care provider under a promise of confidentiality, and the access requested would be likely to reveal the source of the information.

Practice may deny a patient access to health information, provided that the patient is given a right to have such denials reviewed in the following circumstances:

- A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the patient or another person;

- The information makes reference to another person (unless such other is a health care provider), and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; and

- The request for access is made by the patient's personal representative, and a licensed health care professional has determined, in the exercise of

professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the patient or another person.

If access is denied on a reviewable ground, the patient has the right to a review of the denial by a licensed health care professional who is designated by Practice to act as a reviewing official and who did not participate in the original decision to deny access.

If Practice denies the patient's request for access, we will provide a written denial to the patient that contains:

- The basis for the denial;
- A description of the patient's review rights (if applicable); and
- A description of how the patient may complain to Practice, including the telephone number of the Privacy Officer.

_____ _____

Signature Date

Privacy Officer

Practice **POLICY & PROCEDURE** **MANUAL:** Administrative **SECTION:** HIPAA Patient Rights **SUBJECT:** Right to Request Amendment	Policy # HIPAA P-2 Total Pages: 2 Effective Date: Approved:

PURPOSE: To provide guidelines to comply with the HIPAA privacy regulation's requirement to allow patients to request amendments to their protected health information.

POLICY: It is the policy of [Insert Name of Your Practice] to provide patients the right to request amendments to their protected health information.

PROCEDURE:

A patient may request that Practice amend protected health information or a record about the patient in a designated record set for as long as the information is maintained in the designated record set.

Practice will act on a patient's request for an amendment within 60 days of receiving the request. If Practice is unable to act on a request within 60 days, it may extend the time frame by no longer than 30 days by providing the patient with a written statement outlining the reasons for the delay and specifying the date by which action on the request will be completed.

Practice requires a patient to make a request for an amendment in writing and to provide a reason to support this amendment, and will inform the patient in advance of such requirements as part of the Notice of Privacy Practices.

If Practice accepts the requested amendment, it will make the appropriate amendment to the protected health information or record by identifying the records in the designated record set that are affected by the amendment and by appending or otherwise providing a link to the location of the amendment.

Practice will make reasonable efforts to inform and provide the amendment within a reasonable period of time to persons identified by the patient as having received protected health information and as needing the amendment. Practice will also inform and provide the amendment to business associates who possess the protected health information that is the subject of the amendment.

If Practice is informed by another covered entity of an amendment to a patient's protected health information, Practice must amend the protected health information in designated record sets that it maintains.

Practice may deny a patient's request for an amendment if it determines that the protected health information or record that is the subject of the request meets any of the following conditions:

- It was not created by Practice, unless the patient provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;

- It is not part of the designated record set;

- It would not be available for inspection under the regulation; or

- It is accurate or complete.

If Practice denies a request for an amendment, Practice will provide the patient with a denial written in plain language that contains the following:

- The basis for the denial;

- An explanation of the patient's right to submit a written statement disagreeing with the denial and instructions on how the patient may file such a statement;

- A statement that, if the patient does not submit a statement of disagreement, the patient may request that Practice provide the patient's request for an amendment and the denial along with any future disclosures of the protected health information; and a description of how the patient can file a complaint.

Practice may prepare a written rebuttal to the patient's statement of disagreement. Practice must provide a copy of the rebuttal to the patient who submitted the statement of disagreement.

_____ _____

Privacy Officer Date

Practice **POLICY & PROCEDURE** **MANUAL:** Administrative **SECTION:** HIPAA Patient Rights **SUBJECT:** Request Restriction on Use and Disclosure	Policy # HIPAA P-3 Total Pages: 2 Effective Date: Approved:

PURPOSE: The purpose of this policy is to comply with the Privacy Rule Standard that provides patients the right to request a restriction on Use or Disclosure of PHI.

POLICY: Practice will provide its patients with the right to request restrictions on the use and disclosure of protected health information. Practice is not required to agree to a requested restriction. If, however, Practice agrees to a requested restriction, Practice will not use or disclose the information in violation of the restriction, except in an emergency treatment situation as provided in this policy and procedure.

PROCEDURE:

Practice will permit a patient to request a restriction on the use or disclosure of protected health information. All requests must be in writing and must state the information and/or persons subject to the requested restriction. Practice may accept a patient's request for restriction if it determines that all of the following conditions apply:

in the judgment of one of its licensed health care professionals, the restriction will not limit Practice's ability to provide quality health care treatment;

the restriction will not limit Practice's ability to carry out health care operations;

Practice's information management procedures and systems permit consistent compliance with the requested restriction;

the restriction is not effective to limit or prevent uses or disclosures authorized or required by law, as described in Practice's privacy policies and procedures.

Practice will take the following steps to process a request:

verify the patient's identity by comparing the signature on the patient's written request with a sample maintained in the medical record,

place the request in the patient's medical or other record, as applicable, and

route the request to the treating clinician for a recommendation on whether to accept or deny the request

notify the patient and document the decision to accept or reject the request

file original request and the written acceptance in the patient's permanent records such that the request can be honored.

Practice will not use or disclose the patient's protected health information in violation of the requested restriction, unless such use or disclosure is needed to provide emergency treatment Services as provided in this procedure. Practice will take reasonable steps to ensure that any restricted information used or disclosed to provide the emergency treatment is not subject to further use or disclosure

Practice will accept written requests for termination of a restriction at any time and will document the request if made orally by the patient.

Practice may terminate its agreement to restrict a patient's protected health information pursuant to one of the following procedures:

the person agrees to the termination in writing;

the person orally agrees to the termination and the oral agreement is documented; or

Practice informs the patient that it is terminating its agreement to a restriction and the termination is made effective after Practice has informed the patient of the intended termination.

Practice will retain all documentation relating to any restrictions that it accepts, including any terminations of such restrictions, for at least six (6) years or such other period as may be required by Practice' privacy documentation policy and procedure or the Privacy Rule.

_____ _____

Privacy Officer Date

Practice **POLICY & PROCEDURE** **MANUAL:** Administrative **SECTION:** HIPAA Workforce **SUBJECT:** Confidentiality and Security	Policy # HIPAA W-1 Total Pages: 1 Effective Date: Approved:

PURPOSE: The purpose of this policy is to comply with the Privacy Rule Standard that requires covered entities to safeguard PHI from any intentional or unintentional disclosure in violation of Practice policies or procedures.

POLICY: It is the policy of Practice to encourage each member of the workforce to make their best effort to protect the confidentiality of PHI. Recognizing that circumstances will dictate the specific response the situations, each employee shall use their best judgment when using or disclosing PHI, following the policies and procedures that may apply.

PROCEDURE:

Practice will train all staff pursuant to the Training Policy of Practice and at the completion of the training, each participant will sign a Confidentiality Agreement to emphasize the importance of this HIPAA Standard.

The practice will complete an initial risk analysis to identify the business processes and physical / facility that require modification to ensure patient confidentiality. The Privacy Officer will review this analysis and make recommendations as may be reasonably required to address deficiencies.

_____ _____

Privacy Officer Date

Practice **POLICY & PROCEDURE** **MANUAL:** Administrative **SECTION:** HIPAA Workforce **SUBJECT:** Training	Policy # HIPAA W-2 Total Pages: 1 Effective Date: Approved:

PURPOSE: The purpose of this policy is to comply with the Privacy Rule Standard that requires covered entities to train all members of the workforce on the requirements of the HIPAA legislation to the extent necessary for members of the workforce to carry out there responsibilities.

POLICY: Practice will conduct initial and ongoing training to keep it's workforce focused on the importance of the HIPAA legislation, and to review policies and procedures on the use, disclosure, and handling of PHI.

PROCEDURE:

Practice will conduct an initial training session prior to April 14, 2003 to establish an awareness of the legislation and discuss the steps necessary for Practice to comply with the regulations.

New members of the workforce will be provided Privacy Training within the first 10 days of employment; the role and duties within the office will dictate the amount of training needed.

All members of the workforce will sign a confidentiality agreement that will be maintained on file in the HIPAA information binder, and will be required to sign a training log indicating participation in the training session.

Material changes in the policies and procedures of Practice will be reviewed with those members of the workforce whose functions are materially effected, and that review will take place within 10 days of the approval by the practice.

No less than annually, the Privacy Officer will provide the workforce, in person or by written communication, an update on policy or procedure changes, or general information regarding the HIPAA regulations.

Practice will document training sessions, and may choose to administer examinations or use other techniques to help ensure an adequate understanding of the regulations and Practice policies and procedures. Documentation of training will be maintained for 6 years.

Practice will generally require Business Associates to train their personnel on relevant HIPAA standards. However, Practice may choose to conduct such training at its discretion.

_____ _____

Privacy Officer Date

Practice **POLICY & PROCEDURE** **MANUAL:** Administrative **SECTION:** HIPAA Disclosures **SUBJECT:** Uses and Disclosures Policy	Policy # HIPAA D-1 Total Pages: 3 Effective Date: Approved:

PURPOSE: The purpose of this policy is to ensure that our practice and its physicians and staff have the necessary medical and PHI to provide the highest quality medical care possible while protecting the confidentiality of the PHI of our patients to the highest degree possible.

POLICY: It is the policy of our practice that all physicians and staff preserve the integrity and the confidentiality of protected health information (PHI) pertaining to our patients. Practice and its physicians and staff will use PHI for routine disclosures related to treatment, payment and healthcare operations (TPO); our policy for non routine disclosures is to seek patient authorization. Practice will abide by special requests and will not violate the restrictions or accepted requests when it has accepted a restriction of disclosure, or accepted a request for confidential communications.

PROCEDURE:
Routine disclosures for TPO require the reasonable judgment of members of the workforce, and in a manner consistent with our Notice of Privacy Practices. Routine disclosures will be made using our best judgment concerning the minimum necessary amount of information. Example of routine uses and disclosures include but are not limited to:

providing information to pharmacies, consulting physicians, therapists, or to other providers for the treatment activities

supplying information to insurance companies to secure payment for our services

using information for patient reminder or recall systems

using information for data analysis or data aggregation

providing information to another health care provider, or

to a health plan or other entity subject to the requirements of the Privacy Rule, for the payment activities of that provider, health plan or other entity, or

to another health care provider, health plan or other entity for their health care operations activities, provided that both Practice and the other entity have or had a

relationship with the patient, the information disclosed pertains to that patient relationship, and the disclosure is for one of the following purposes or activities:

conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers with information about treatment alternatives, and related functions that do not include treatment;

reviewing the competence or qualification of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting professional and non-professional training programs, accreditation, certification, licensing, or credentialing activities;

health care fraud and abuse detection or compliance.

Using information for the following marketing activities:

a face-to-face communication between a member of Practice's workforce and a patient

a promotional gift of nominal value provided by Practice

Practice will obtain a valid authorization for all other marketing uses or disclosures.

Making disclosures to the individual

Disclosing information for law enforcement, public health, or other permitted disclosures identified in the regulations

Providing information to Business Associates with whom Practice has a written agreement; examples of reasons for PHI to be disclosed to a Business Associate include:

billing, claims processing or administration
data analysis processing or administration
utilization review or quality assurance
medical transcription
practice management

Practice will also make determinations on requests for non routine disclosures on an individual basis pursuant to authorization, and those disclosures shall be consistent with the Minimum Necessary policies and procedures of the practice. Examples of non routine disclosures include but are not limited to:

disclosures to life insurance companies for health information

disclosures to schools for maintaining immunization records

disclosures to employers requesting information related to employment opportunities

The minimum necessary requirements for non routine disclosures will not apply to:

disclosures to or requests by a health care provider for treatment purposes.
authorized or required disclosures to a patient or a patient's representative.
uses or disclosures made pursuant to a valid authorization when the authorization is initiated by the patient or the patient's representative.
uses or disclosures to the Secretary of DHHS for enforcing the Privacy Rule.
uses or disclosures required by law.
uses or disclosures that are required for compliance with the regulations implementing the other administrative simplification provisions of HIPAA.

Such disclosures will be maintained in a log of non routine disclosures that will be made available to patients upon written request consistent with Practice's policies and procedures.

If a member of the workforce has any doubt as to whether the disclosure requires authorization, he/she should consult with the practice Privacy Officer.

_____ _____

Privacy Officer Date

Practice **POLICY & PROCEDURE** **MANUAL:** Administrative **SECTION:** HIPAA Disclosure **SUBJECT:** Minimum Necessary	Policy # HIPAA D-2 Total Pages: 1 Effective Date: Approved:

PURPOSE: The purpose of this policy is to comply with the intent of the Privacy Rule requires covered entities to limit the use and disclosure of PHI to the minimum necessary to accomplish the stated purpose.

POLICY: Practice will make its best effort to identify those persons or classes of persons in the workforce who need access to PHI to carry out their duties, specify the categories of information required, and make reasonable efforts to limit access consistent with the classes and categories defined.

PROCEDURE:

Practice will emphasize the importance of professional judgment when implementing the minimum necessary standard, until such time that the Privacy Officer has identified the classes and categories of the workforce to provide more detailed guidance in order to comply with the Minimum Necessary Policy. That guidance will be appended as an attachment to this Policy.

Practice recognizes the following exemptions to the Minimum Necessary requirement:

- Disclosures to or requests by a health care provider for treatment
- Uses or disclosures of PHI made to the individual, including upon the individual's request for access to PHI or for and accounting of disclosures
- Disclosures made pursuant to an authorization
- Disclosures made to the secretary of HHS for purposes of compliance and enforcement related to the HIPAA Privacy Rule
- Uses of Disclosures that are required by law
- Uses or disclosure that are required for compliance with applicable requirement of the HIPPAA administrative simplification provisions, including the Privacy Rule, the Transaction Rule, and the Security Rule (when in its final form)

Members of the Workforce who receive a request for "any and all" records should refer the request to the Privacy Officer for further assessment prior to responding to the request.

_____ _____

Privacy Officer Date

Practice **POLICY & PROCEDURE** **MANUAL:** Administrative **SECTION:** HIPAA Disclosure **SUBJECT:** Psychotherapy Notes	Policy # HIPAA D-3 Total Pages: 2 Effective Date: Approved:

PURPOSE: The purpose of this policy is to comply with the Privacy Rule Standard that requires covered entities to safeguard the use and disclosure of psychotherapy notes.

POLICY: It is the policy of Practice to recognize the special nature of psychotherapy records and to exclude these records from routine disclosure of PHI.

DEFINITION:
For the purpose of this procedure, psychotherapy notes means the notes recorded by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the patient's medical record.

PROCEDURE:
Practice will [describe how these records are maintained separately and how access is restricted]

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Practice will use and disclose psychotherapy notes for any one of the following types of treatment or health care operations:

for treatment purposes by the health care professional who created the notes

for uses and disclosures by Practice for its own training programs in which students, trainees or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling

for uses or disclosures by Practice to defend a legal action or other proceeding brought by the patient

for uses and disclosures required by law or otherwise permitted without the patient's authorization as described in Practice' policies and procedures governing mandatory releases.

Practice will obtain a valid authorization for all other releases of psychotherapy notes. No authorization is required for medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of a patient's diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.

_____

Privacy Officer Date

FORMS

EMBED Word.Document.8 \s EMBED Word.Document.8 \s EMBED Word.Document.8 \s

Patients' Request to File a Complaint

I wish to file a complaint to the Practice Privacy Officer regarding a possible violation of your privacy policies.

My Name: _____

Please Contact me at the following address / telephone number:

_____

_____

_____

Please describe the nature of your concern and specific details such as the names of those involved, dates, times, and places:

_____

_____

_____

_____

_____

_____

Please share your thoughts on actions that you feel are appropriate to address your concern:

_____

_____

_____

_____ _____

Patient Signature Date

BUSINESS ASSOCIATE AGREEMENT
(Privacy Standards Only)

THIS AGREEMENT, made and entered into this _____ day of _____, 200__, by and between Practice, hereinafter to as "Healthcare Provider", and (Business Associate), Hereinafter referred to as "Business Associate".

WITNESSETH:

DEFINITIONS:

Business Associate. "Business Associate" shall mean (Name of the Business Associate).

(b) Covered Entity. "Covered Entity" shall mean (Name of Health Care Provider).

(c) Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502 (g).

(d) Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

(e) Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(f) Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR 164.501.

(g) Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE:

Business Associate agrees to not use or disclose Protected Health Information other then as permitted or required by the Agreement or as Required By Law.

Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

Business Associate agrees to ensure that any agent, including a subcontractor, to whom it

provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

Business Associate agrees to provide access, at the request of Covered Entity, and in the following time and manner. (To be agreed between the parties and inserted here.); to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524.

Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in the following time and manner (To be agreed between the parties and inserted here).

Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created Covered Entity, or to the Secretary, in a time and manner [Insert negotiated terms] or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

Business Associate agrees to provide to Covered Entity or an Individual, in the following time and manor [Insert negotiated terms], information collected in accordance with the foregoing Subparagraph (i) of the Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

PERMITTTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in that certain Agreement now existing between the Parties, Provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

Specific Use and Disclosure Provisions:

Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provide that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 CFR 164.504 (e)(2)(i)(B).
Business Associate may use Protected Health Information to report-violations of law to appropriate Federal and State authorities, consistent with Sec. 164.502 (j)(I).

OBLIGATIONS OF COVERED ENTITY

Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.
Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclosure Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.
Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

PERMISSABLE REQUESTS BY COVERED ENTITY

> Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity; Provided, However, Business Associate may use Protected Health Information for the proper management and administration of the Business Data Aggregation services to Covered Entity as permitted by 42 CFR 164.504(e)(2)(i)(B).

TERM AND TERMINATION

Term The Term of the Agreement shall commence on the date hereof, and shall terminate only when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity is destroyed of returned to the Covered Entity. If it is infeasible to destroy or return Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this section.

Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

Provide an opportunity for Business Associates to cure the breach or end the violation, and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity.
Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or
If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary.

Effect of Termination.

Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any

reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

MISCELLANEOUS

Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

Survival. The respective rights and obligations of Business Associate under Section VI. (C) of this Agreement shall survive the termination of this Agreement.

Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

Governing Law. This Agreement shall be construed broadly to implement and comply with the requirement relating to the HIPAA laws and regulations. All other aspects of the Agreement shall be governed under the laws of the State of <Name State> and venue for any actions relating to this Agreement shall be proper in <County, State>.

IN WITNESS WHEREOF, the Parties hereto have affixed their signatures on the day and year first above written.

_____ _____

(Business Entity) (Business Associate)

PRACTICE

WORKFORCE CONFIDENTIALITY AGREEMENT

I understand that Practice has a legal and ethical responsibility to maintain patient privacy, including obligations to protect the confidentiality of patient information and to safeguard the privacy of patient information.

In addition, I understand that during the course of my employment/ assignment /affiliation at Practice I may see or hear other Confidential Information such as financial data and operational information pertaining to the practice that Practice is obligated to maintain as confidential.

As a condition of my employment/assignment/affiliation with Practice, I understand that I must sign and comply with this agreement.

By signing this document I understand and agree that:

I will disclose Patient Information and/or Confidential Information only if such disclosure complies with Practice policies, and is required for the performance of my job.

My personal access code(s), user ID(s), access key(s) and password(s) used to access computer systems or other equipment are to be kept confidential at all times.

I will not access or view any information other than what is required to do my job. If I have any question about whether access to certain information is required for me to do my job, I will immediately ask my supervisor for clarification.

Recognizing the difficulty presented by the physical layout of our facility, I will use professional judgment and make my best effort not discuss any information pertaining to the practice in an area where unauthorized individuals may hear such information. I understand that it is not acceptable to discuss any practice information in public areas even if specifics such as a patient's name are not used.

I will not make inquiries about any practice information for any individual or party who does not have proper authorization to access such information.

I will not make any unauthorized transmissions, copies, disclosures, inquiries, modifications, or purgings of Patient Information or Confidential Information. Such unauthorized transmissions include, but are not limited to, removing and/or transferring Patient Information or Confidential Information from Practice's computer system to unauthorized locations (for instance, home).

Upon termination of my employment/assignment/affiliation with Practice, I will immediately return all property (e.g. keys, documents, ID badges, etc.) to Practice.

I agree that my obligations under this agreement regarding Patient Information will continue after the termination of my employment/ assignment/ affiliation with Practice.

I understand that violation of this Agreement may result in disciplinary action, up to and including termination of my employment/assignment/affiliation with Practice and/or suspension, restriction or loss of privileges, in accordance with Practice's policies, as well as potential personal civil and criminal legal penalties.

I understand that any Confidential Information or Patient Information that I access or view at _____ does not belong to me.

I have read the above agreement and agree to comply with all its terms as a condition of continuing employment.

Signature of employee/physician/student/volunteer		Date
Print Your Name		

Dr. Mendy Maccabee