Policy and Procedure Manual for HIPAA Privacy - 2023

POLICIES FOR MANAGEMENT AND PROTECTION OF PROTECTED HEALTH INFORMATION (PHI)

GENERAL PRIVACY POLICY: To the extent possible, Lauren Penner Therapy, PLLC will prevent any harmful effect resulting from the use or disclosure of personal health information (PHI) in a way that violates Federal law or the privacy policies of this practice. PHI is information, including demographic information, that may identify the patient, that relates to provided health care services, the payment of health care services, or the patient's physical or mental health or condition, in the past, present or future. Designated health records include written and electronic patient charts, session notes, billing information, demographic Information and forms that contain patient's PHI. This does not include psychotherapy notes or de-identified information used for consultation or education.

Privacy officer is Lauren Penner, LPC #86371

MINIMUM NECESSARY RULE: HIPAA requires that disclosures and uses of PHI be limited to the minimum amount of PHI needed to complete the function for which the PHI is being used or disclosed. Plan: -All uses and disclosures of PHI, will be limited to the minimum necessary amount of PHI to complete the task. When possible and appropriate, de-identified data will be used in place of PHI. -Access to PHI, electronic and paper, will be limited according to position and the need needed access. Procedures will be followed for disclosures of PHI, including verifying that the party has necessary agreements for access (Business Associate Agreement, Authorization to Obtain and/or Release Protected health information, etc.) signed and on file prior to making the disclosure. -All non-standard requests for disclosure of PHI will be reviewed by the Privacy Officer to determine if disclosure is appropriate and if any agreements are necessary prior to making the disclosure.

1. IDENTITY/AUTHORITY VERIFICATION: HIPAA requires that prior to disclosing PHI the identity of the requester and that person's authority to have access to the PHI is verified. Plan: -Disclosures of PHI will not be made in any format – verbal, written or electronic – until the identity of the person making the request and their authority to access the information has been verified through the following information (information provided must match patient records): -Patient's name (First, Last) -Patient's Date of Birth -The requester's name and relationship to the patient if not the patient -If required, written authorization for release of PHI will be obtained prior to making any disclosures -Authorization to request disclosure will be determined based on the following guidelines: -Adult Patients – allowed access to their own PHI only -Minor/Dependent

child (under 18) – not allowed access without written/signed Authorization from the guardian -Personal Representative (designated by written/signed authorization) – Allowed access to patient's PHI -Business Associate – allowed access with a signed Business Associate Agreement on file -Custodial Parent – allowed access to PHI for dependent child (must be supported be legal documentation in case of separation, divorce or other custody situations) -When requests are made by someone other than the patient or their personal representative the information disclosed will be determined based on the requester's authority to information, written authorization dictating what information is permitted by the patient for release, or information needed to create safety and respond to emergency situations. -PHI will only be sent to the address or fax listed in patient records, or through secure electronic means. If the individual request is we use a different address, fax number, or secure email, the new information must be verified by the patient verbally or in writing.

2. DISCLOSURE TO BUSINESS ASSOCIATES: Plan: -Protected health information (PHI) will not be disclosed to a Business Associate unless a signed Business Associate Agreement is in place. -If a signed agreement is not in place, the Privacy Officer will determine whether a Business Associate Agreement is appropriate and send an agreement to be signed prior to release of PHI -If the Privacy Officer determines that there is not a need to share PHI with the entity, the Privacy Officer will respond that PHI cannot be released to the entity.

3. PERSONAL REPRESENTATIVE: HIPAA requires that representatives of a patient be treated as if they were the patient when: -The representative has legal standing to act on behalf of the patient who is an adult or emancipated child. -The representative is the parent or guardian of the patient who is a minor child. - The representative is the executor or administrator of the deceased patient or the deceased patient's estate. Plan: -Authority of the person to act as a personal representative will be verified as follows: -Personal Representative of Adult or Emancipated Child -One of the following forms of authority must be provided: 1. Designation of Authorized Representative Form 2. Executed copy of Power of Attorney. 3. Copy of court order giving authority. 4. Personal Representative of Minor Child 5. Name matches parent or step-parent. 6. Guardianship papers are provided. 7. Personal Representative of Deceased Patient 8. A copy of the will or court papers designating the representative as the executor or administrator. -Once authorization has been verified, access to the patient's PHI will be provided to the personal representative to the same extent that access would be provided to the patient.

4. REQUEST TO RESTRICT USES & DISCLOSURES: HIPAA guarantees all patients the right to request restrictions on how their PHI is used and disclosed. Plan: -General Requests to Restrict Uses and Disclosures of PHI -All requests to limit the use or disclosure of PHI must be in writing and submitted to the Privacy Officer. -The Privacy Officer will review the request to determine whether the requested restrictions are appropriate and/or possible. Reasonable efforts will be made to accommodate requests. -The Privacy Officer will respond to the request in writing and/or by phone, within 15 days of receipt of the request. -Any denial of requests will be explained in writing. -The request and response will become part of the patient's file and will be maintained as defined by state law. -If

the request for alternate means of communication or location cannot be accommodated, a reasonable alternative will be offered. -Requests to Provide PHI by Alternate Means or Location -All requests to provide PHI by an alternate means or location must be submitted in writing to the Privacy Officer for review. -The Privacy Officer will determine whether the request is reasonable and possible, and will respond in writing and/or by phone, within 15 days of receipt of the request. -Denial of any requests will be explained in writing. -The request and response will become part of the patient's file and will be maintained as defined by state law.

5. AUTHORIZATION: An authorization is permission from the patient to use or disclose their (PHI) for a specific purpose. Under HIPAA, an authorization must contain specific provisions that have been included in the Authorization to Obtain and/or Release Protected Health Information form. -HIPAA does not require that an authorization be obtained for the following uses and disclosures of PHI: -Those made in carrying out the functions of payment and health care operations, except for medical records requests for psychotherapy notes. -Those made to health oversight agencies, such as the DOL, IRS and OCI. -Those made in relation to legal hearings. *Providers are not required to release PHI without a signed HIPAA Authorization and may request such an authorization, even if it may not be required by law for the indicated use or purpose. Plan: -The Authorization to Obtain and/or Release Protected Health Information form will be completed and signed by the patient in all cases where authorization is required prior to use or disclosure of PHI -If medical records, letters or other documentation containing PHI are requested, the signed authorization form will be attached and sent along with the requested information -The signed authorization will become part of the patient's file and will be maintained as defined by state law. -The authorization form may also be used to accommodate requests by the patient to disclose PHI to third parties, such as a parent, other providers, attorneys, etc.

6. REQUEST TO ACCESS PROTECTED HEALTH INFORMATION: HIPAA guarantees all patients the right to obtain a copy of or review their PHI, as maintained in a designated record set, for as long as the information is maintained. Records subject to inspection include: -All materials kept as the patient's treatment records including session notes, documented correspondence and consultation, letters prepared regarding client's treatment, diagnosis, materials received from other providers, billing information, payment statements, etc. *Psychotherapy notes or de-identified material is not included. Plan: -All requests for PHI access must be submitted in writing to the Privacy Officer. -The Privacy Officer will review the form and determine whether the request will be accepted or denied. -Access will only be denied if it is determined that the requested information: 1. Is not in our files. 2. Is psychotherapy notes. 3. Was compiled for use in a legal proceeding. 4. Is subject to the Privacy Act (5 USC 552a) dealing with information held by or on behalf of a federal government agency or affiliated non-federal agency and denial is allowed under that Act. 5. Is likely to endanger or cause substantial harm to the patient or another person, according to a decision by a licensed health care professional. (An appeal of the decision must be allowed.) -If the request is approved, the appropriate files be printed and/or copied and mailed or handed to the patient within 15 days of receiving the request. -Denials will be explained in writing and patient

can appeal decision. -Any appeals to denial will be received in writing by the Privacy Officer and further action will be determined. -The request and response will become part of the patient's file and will be maintained as defined by state law.

7. REQUEST TO AMEND PROTECTED HEALTH INFORMATION: HIPAA guarantees patients the right to have their PHI, as maintained in a designated record set, amended if it is incorrect. Records subject to amendment include: -Insurance Information -Demographic Information -Contact Information -Session notes Plan: -Requests may come from patients or other covered entities -Privacy Officer will verify authority to request amendment -All requests to amend PHI must be submitted in writing to the Privacy Officer. -The Privacy Officer will review and determine whether the request will be accepted or denied -Requests to amend PHI will only be denied if it is determined that: 1. The clinician did not create the information and is not responsible for the incorrect data. 2. The information is not part of a designated record set listed above. 3. The clinician is not required to make the information available to the patient for inspection. 4. The information is accurate and complete as stated in the record. -The Privacy Officer will respond in writing and/or by phone to the patient within 15 days of receipt of the request for amendment. -If the request is being accepted, the Privacy Officer will: 1. Identify the records affected by the amendment and request that the amendment be included or linked to those records. 2. Amend incorrect data and document reason for amendment. 3.3 Provide written notice of the amendment to any person listed as requiring notification of the amendment. 4. Provide written notice of the amendment to any Business Associate or anyone who was provided the original information and who may rely on it to detriment of the individual. -If a rebuttal to a denial is received, the Privacy Officer will document receipt and determine further action. -All future disclosures of information that are associated with a request for amendment, whether accepted or denied, will include the request for amendment, the decision on the request, and any rebuttal to the decision. -The request, response and any rebuttal will become part of the individual's file and will be kept as defined by state law.

8. REQUEST FOR ACCOUNTING OF DISCLOSURES: HIPAA guarantees every individual the right to a listing or accounting of the disclosures of their PHI for a period of up to 6 years prior to the request, with the exception of disclosures made: -To carry out the functions of treatment, payment and health care operations. -Under a signed HIPAA Authorization. -To the patient themselves. -That is incidental to a use or disclosure otherwise permitted under the regulation. -As part of a limited data set. -To persons involved in the patient's care or for notification purposes. -For national security or intelligence purposes. -To correctional institutions or law enforcement officials. -Business management and general administrative activities of the entity. Plan: -An accounting of disclosures of PHI will not be made if the disclosures fall within the exceptions listed above. -All requests for accounting must be in writing and received by the Privacy Officer. -The Privacy Officer will respond in writing and/or by phone to the individual within 15 days of receipt of the request. -The request and response will be maintained as defined by state law.

9. BREACH OF PHI NOTIFICATION: HIPAA requires that individuals be notified if unsecured PHI has been breached.
Plan: -The Privacy Officer will be notified of any possible breach of unsecure PHI the Privacy Officer will immediately conduct a risk assessment -The Risk assessment can be done by a business associate if it was involved in the breach. While the business associate can conduct a risk assessment, the Privacy Officer will provide any required notice to patients and HHS. -The Risk Assessment will determine: -The nature and extent of the PHI involved -To whom the PHI may have been disclosed -Whether the PHI was actually acquired or viewed -The extent to which the risk to the PHI has been mitigated -Was the PHI unsecure -The steps and results of the Risk Assessment will be documented -If it is determined that there is a low probability that the PHI has been compromised, no notification will occur -If it is determined there is probability that the PHI has been compromised and was unsecure -The Privacy Officer will notify any patient affected by the breach without unreasonable delay and within 60 days after discovery. The notice will include: A. Brief description of the breach, including dates B. Description of types of unsecured PHI involved C. The steps the patient should take to protect against potential harm D. Brief description of steps taken to investigate the incident, mitigate harm, and protect against further breaches E. Contact information for the Privacy Officer

Breaches affecting 500 patients or more will be reported to HHS and major media outlets as dictated by law.

1. PRIVACY COMPLAINT PROCESS:
Plan: -The privacy officer, Lauren Penner, LPC #86371 is responsible for receiving, responding to, and documenting all privacy complaints. -Complaints must be submitted in writing. -The complaint will be researched to determine the validity. -If the complaint is valid, the Privacy Officer will determine if mitigation of any harm is appropriate and possible. -The Privacy Officer will respond to the complaint in writing within 15 days. -The Privacy Officer will maintain and document the complaint, any information collected in researching it, and the final response to it as defined by state law.

2. PRIVACY NOTICE QUESTIONS AND INFORMATION:
Plan: -The privacy officer will respond to any inquiries regarding the Notice of Privacy Practices by providing the requested information within 15 days of receipt of the inquiry, which must be submitted in writing.

3. ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS: Plan: - Appropriate administrative, technical and physical safeguards will be followed to ensure the protection of information received, maintained, and disclosed, as required by HIPAA. -Safeguards will account for the nature of the information, where it is located, and its various formats and media. -Physical safeguards: -All paper files will be secured in a locked file cabinet inside a locked office during non-working hours. Access will be limited to this clinician and the business associate. -Fax machines will be secured in a locked hallway during non-working hours. Access will be limited to clinicians and business associate. -All electronic transmissions will include a statement of confidentiality, or be transmitted through secure encrypted means. -All printed material containing PHI will be placed in envelopes in such a way that no PHI is visible. -All paper

documents containing PHI will be shredded prior to disposal for recycling. -Material containing PHI will not be left unattended in common areas such as copy rooms, break rooms, in suite bathroom, or break room. -Technical safeguards: -Clinician's laptop will be stationed where the screen is not visible to any but the clinician and clinician will close programs with access to PHI or use blocking screen savers before anyone approaches the desk. -Clinician's laptop and all files will have password protection to prevent unauthorized access to data on the laptop. -Clinician's cell phone or any other devices used to communicate with clients will be kept out of sight or reach of others who do not have authorization to access PHI -Confidential information on devices will be protected by passwords -Thumb drive containing PHI will be stored in a locked safe in locked file cabinet and will be transported in a locked safe. -Administrative safeguards: -Clinician will participate in yearly training on Federal and State Privacy and Security rules/laws and will ensure that business associate, and employees have adequate training as well. -Certificates that document dates of training will be kept for 6 years. -Transport and disposal of all media types (external drives, emails, laptops, etc.) will conform to appropriate methods to ensure that PHI is removed and no longer accessible. -Access to PHI in electronic systems will be limited to clinician and business associate with only minimum information necessary accessible to perform duties. -Clinician will not disclose PHI in any format or manner (electronic, paper, or verbal) except as necessary for business reasons and in compliance with the Minimum Necessary rule. This includes external and internal disclosures.