



Lindsay Martin, PhD, LPC, NCC

Licensed Professional Counselor

lindsay@drlindsaymartin.com

www.drlindsaymartin.com

NOTICE OF COUNSELOR'S POLICIES AND PRACTICES TO PROTECT THE PRIVACY OF YOUR HEALTH INFORMATION

THIS NOTICE OF PRIVACY PRACTICES ("NOTICE") DESCRIBES HOW PSYCHOLOGICAL AND MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

PURPOSE

I am required by law to maintain the privacy of your health information. This Notice describes my legal duties and privacy practices and how I may use and disclose your health information. This Notice also describes your rights and how you may exercise your rights. I agree to abide by the terms of this Notice.

Your Protected Health Information. "Protected Health Information" or "PHI" is health information that I have collected in my records from you or received from other health care providers. It may include information about your past, present or future physical or mental health or condition. For example, PHI in your records could include your diagnosis, treatment plan, or evaluations. PHI also includes information about payment for services.

Confidentiality of Your PHI. Your PHI is confidential. I am required to maintain the confidentiality of your PHI by the following federal and Pennsylvania laws.

- **The Health Insurance Portability and Accountability Act of 1996.** The U.S. Department of Health and Human Services issued the following regulations: "Standards for Privacy of Individually Identifiable Health Information." This document refers to these regulations as the "HIPAA Privacy Regulations." I may not use or disclose your PHI except as required or permitted by the HIPAA Privacy Regulations. The HIPAA Privacy Regulations require me to comply with Pennsylvania laws that are more stringent and provide greater protection for your PHI.
- **Pennsylvania Mental Health Confidentiality Laws.** Pennsylvania laws may provide greater protection for your PHI than the HIPAA Privacy Regulations. For example, I am not permitted to disclose or release PHI in response to a Pennsylvania subpoena. Also, any information acquired by a licensed counselor in the course of treatment is privileged under Pennsylvania law and may not be released without client/patient authorization or court order. Finally, if mental health records include information relating to drug or alcohol abuse or dependency, I am required to comply with the Pennsylvania Drug and Alcohol Abuse Control Act. I will comply with the Pennsylvania laws that are more stringent than the HIPAA Privacy Regulations and provide greater protection for your PHI.

Why this Notice is Important. The HIPAA Privacy Regulations require that I provide you with this Notice. A current copy of the Notice will be posted at my office and on the practice website: www.drlindsaymartin.com. A copy of our Notice is available upon request. I reserve the right to change the terms of this Notice at any time. The revised Notice will be posted in the office, the practice website, and available to you upon request.

AUTHORIZATION TO DISCLOSE YOUR PHI

Except as described in this Notice, it is my practice to obtain your authorization before I disclose your PHI to another

person or party. Pennsylvania law states that you are entitled to inspect the PHI that is contained in my records. You may revoke an authorization, at any time, in writing. If you revoke an authorization, I will no longer use or disclose your PHI. However, I cannot undo any disclosures I have already made.

HOW I MAY USE OR DISCLOSE YOUR PHI WITHOUT YOUR AUTHORIZATION

Uses and Disclosures for Treatment, Payment, and Health Care Operations.

Unless prohibited by more stringent Pennsylvania laws, the HIPAA Privacy Regulations permit me to use and disclose your PHI for the following purposes in order to provide your treatment:

For Treatment. I may disclose your PHI to physicians, psychiatrists, psychologists, and other licensed health care providers who provide you with health care services or are otherwise involved in your care. For example, if a psychiatrist is treating you, I may disclose your PHI to him/her in order to coordinate your care. When you are referred to another provider, I am permitted to provide your PHI if it is necessary for the continuity of your care and treatment.

For Payment. I may use and disclose your PHI to obtain payment for services. I may disclose PHI to your insurance company, health plan, other third-party payer to permit them to make a determination of eligibility or coverage; review the medical necessity of your services; review your coverage; or review the appropriateness of care or our charges. I may also use your PHI for billing, claims management, collection activities, and data processing. For example, a bill may be sent to you or whomever pays for your services.

For Health Care Operations. I may use and disclose your PHI within the practice to carry out health care operations. For example, your PHI may be used for business management and general administrative duties; quality assessment and improvement activities; medical, legal, and accounting reviews; business planning and development; and licensing and training.

Business Associates: I may contract with certain outside persons or organizations to perform certain services on my behalf, such as auditing, accreditation, legal services, etc. At times it may be necessary for me to provide your PHI to one or more of these outside persons or organizations. In such cases, I require these business associates, and any of their subcontractors, to appropriately safeguard the privacy of your information.

Other Uses and Disclosures include contacting you to provide appointment reminders or to provide information about treatment alternatives.

Uses and Disclosures That May Be Made Without Your Authorization, But Subject to Your Opportunity to Agree or Object.

Your Opportunity to Agree or Object to Certain Uses and Disclosures. It is my practice to obtain your written authorization prior to disclosing PHI to another person or party. However, as described in this section, it may be necessary to disclose your PHI without your written authorization. Under these circumstances, the HIPAA Privacy Regulations permit me to use or disclose PHI when you are present and have the capacity to make health care decisions if, prior to the use or disclosure, I obtain your agreement, provide you with an opportunity to object (and you do not express an objection), or I can reasonably infer from the circumstances, based upon my professional experience, that you do not object. If you are not present or the opportunity to obtain your agreement or objection cannot practicably be obtained as a result of your incapacity or an emergency, then I may determine in the exercise of professional judgment whether the disclosure is in your best interests and, if so, disclose only PHI that is directly relevant to that person's involvement in your case.

Family Members and Others Involved in Your Healthcare. Subject to your opportunity to agree or object, I may share your PHI with a family member, other relative, close personal friend, or any other person whom you identify (your "personal representative"). The PHI shared with your personal representative will be directly relevant to your personal representative's involvement with your care or payment for services. For example, your personal representative may act on your behalf by picking up forms for you.

Notification. Subject to your opportunity to agree or object, I may use or disclose PHI to notify, or assist in the notification of (including identifying or locating), a personal representative of your location, general condition, or death.

Disaster Relief. Subject to your opportunity to agree or object, I may use or disclose your PHI to a public or private entity (e.g., the American Red Cross) authorized by law or by its charter to assist in disaster relief efforts. The purpose of such use or disclosure of your PHI is to coordinate with a disaster relief agency and/or your personal representative your location, general condition, or death. Only specific information pertinent to the relief effort and the emergency may be released without your authorization.

Other Permitted and Required Uses and Disclosure That May Be Made Without Your Authorization.

Unless prohibited by more stringent Pennsylvania laws, the HIPAA Privacy Regulations permit us to use or disclose your PHI without your authorization or agreement under the following circumstances:

As Required By Law. I will disclose PHI about you when required to do so by federal or Pennsylvania law. Any use or disclosure must comply with and be limited to the relevant requirements of the law. For example, I am required to report or disclose PHI related to child or elder abuse or neglect and commitment proceedings authorized by the Pennsylvania Mental Health Procedure Act of 1966.

Child Abuse: If I have reason to suspect, on the basis of my professional judgment, that a child is or has been abused, I am required to report my suspicions to the authority or government agency vested to conduct child abuse investigations. I am required to make such reports even if I do not see the child in my professional capacity. I am mandated to report suspected child abuse if anyone aged 14 or older tells me that he or she committed child abuse, even if the victim is no longer in danger. I am also mandated to report suspected child abuse if anyone tells me that he or she knows of any child who is currently being abused.

Adult and Domestic Abuse: If I have reasonable cause to believe that an older adult is in need of protective services (regarding abuse, neglect, exploitation or abandonment), I may report such information to the local agency which provides protective services.

Judicial or Administrative Proceedings: If you are involved in a court proceeding and a request is made about the professional services, I provided you or the records thereof, such information is privileged under state law, and I will not release the information without your written consent, or a court order. The privilege does not apply when you are being evaluated for a third party or where the evaluation is court ordered. You will be informed in advance if this is the case. Pennsylvania law requires me to make a good faith effort to notify you by certified mail at your last known address that I disclosed your PHI pursuant to a court order.

Emergencies. I may use or disclose your PHI in an emergency treatment situation when use and disclosure of the PHI is necessary to prevent serious risk of bodily harm or death to you.

Public Health Activities. If required by federal or Pennsylvania law, I will disclose your PHI for public health activities in order to: prevent disease, injury or disability; report births and deaths; report child abuse or neglect; report reactions to medications; notify a person who may be at risk for contracting or spreading a disease or condition; or notify appropriate government authorities if I believe a client/patient has been the victim of abuse, neglect, or domestic violence, when required to do so by law or with your agreement. Only specific information required by law may be disclosed without your authorization.

Health Oversight Activities. If required by law, I may use or disclose PHI about you to a health oversight agency. Oversight activities include audits, accreditation, investigations, inspections, utilization review, and licensure.

To Avert a Serious Threat to Health or Safety. The HIPAA Privacy Regulations permit me to use and disclose PHI about you when necessary to prevent a serious and imminent threat to your health or safety or to the health or safety of the public or another person. Under these circumstances, I will only disclose health information to someone who is able to help prevent or lessen the threat. If you express a serious threat or intent to kill or seriously injure yourself or an identified or readily identifiable person or group of people, and I determine that you are likely to carry out the threat, I must take reasonable measures to prevent harm. Reasonable measures may include directly advising the potential victim of the threat or intent or referring you to a higher level of care. Further, if you are a potential danger to yourself and the public

because of driving while intoxicated and unwilling to make alternate arrangements, I may notify the police.

Law Enforcement Activities. I am not permitted by Pennsylvania laws to disclose PHI regarding mental health or drug and alcohol services to law enforcement agencies or officials except pursuant to a court order or in special circumstances required by law. For example, I may disclose the minimum necessary PHI to report a death or criminal conduct on our premises.

Special Situations. I am not permitted by federal or Pennsylvania laws to disclose PHI regarding mental health or drug and alcohol services except pursuant to the following: your authorization; a court order; medical personnel in a medical emergency; qualified personnel for research, audit or program evaluation; or special circumstances required by federal or state laws. Subject to these more stringent federal or Pennsylvania laws, the HIPAA Privacy Regulations permit me to disclose PHI related to military and veterans agencies; national security and protective services for the President and others; inmates or if you are under the custody of a law enforcement official; a coroner or medical examiner to identify a deceased person or determine the cause of death; or to a funeral director as necessary to carry out their duties.

YOUR RIGHTS REGARDING YOUR PHI

Right to Request Restrictions. You have the right to request a limitation or a restriction on my use or disclosure of your PHI for treatment, payment, or healthcare operations. You may also request that I limit the PHI I disclose to family members, friends or a personal representative who may be involved in your care. However, I am not required to agree to a restriction. If I agree to the requested restriction, I may not use or disclose your PHI in violation of that restriction unless it is needed to provide emergency treatment. You may request a restriction by making your request in writing, including: (a) what PHI you want to limit; (b) whether you want me to limit my use or disclosure or to limit both; and (c) to whom you want the limits to apply.

Right to Request Confidential Communication. You have the right to request that confidential communications from me be sent to you in a certain way or to an alternative location. For example, you can ask that I only contact you at your home or by mail. I will accommodate reasonable requests. I may also condition this accommodation by asking you for specific information. I will not request an explanation from you as to the basis for the request. Please make this request in writing specifying how or where you wish to be contacted.

Right to Inspect and Copy. You have the right to inspect and obtain a copy of your PHI that is contained in practice records. However, you may not inspect or copy the following records: psychotherapy notes or information compiled in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding. In addition, you may be denied access to your PHI if it was obtained from a person under a promise of confidentiality or disclosure is likely to endanger the life and physical safety of you or another person. A decision to deny access may be reviewed. To inspect and copy your PHI, submit your request in writing. If you request a copy of the information, I may charge a fee for the costs of copying, mailing, or other related costs.

Right to Amend. If you believe the PHI that I have collected about you is incorrect, you have certain rights. You have the right to submit a written statement qualifying or rebutting information in practice records that you believe is erroneous or misleading. This statement will accompany any disclosure of your records. You also have the right under the HIPAA Privacy Regulations to request an amendment of the PHI maintained in practice records. I may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, I may deny your request if you ask me to amend information contained in your PHI that was not created by me (unless the person or entity that created the information is no longer available to make the amendment); is not part of the record kept by me; is not subject to inspection or copying; or is accurate and complete. If I deny your request for amendment, you have the right to appeal the decision and file a statement of disagreement with me. I may prepare a rebuttal to such statement and provide you with a copy of any such rebuttal.

Right to Receive an Accounting of Disclosures. You are entitled to a list of disclosures of your PHI that I have made. The list

will not include uses or disclosures to which you have already consented (i.e., those for treatment, payment, or health care operations, sent directly to you or to your family/personal representative); neither will the list include disclosure made for national security purposes or to corrections or law enforcement personnel. I will respond to your request for an accounting of disclosures within 60 days of receiving your request. The list I give you will include disclosures made in the previous six years unless you indicate a shorter period. The list will include the date of the disclosure, to whom PHI was disclosed (including their address, if known), a description of the information disclosed, and the reason for the disclosure.

I will provide the list to you at no cost, unless you make more than one request in the same year, in which case I will charge you a reasonable sum based on a set fee for each additional request.

Right to a Paper Copy of this Notice. You have the right to receive a paper copy of this Notice upon request. This Notice can also be found on the practice website: <https://www.dr.lindsaymartin.com>.

Right to Restrict Disclosures. You have the right to restrict certain disclosures of PHI to a health plan when you pay out-of-pocket in full for my services.

Right to Be Notified if There is a Breach of Your Unsecured PHI. You have a right to be notified if: (a) there is a breach involving your PHI (i.e., a use or disclosure of your PHI in violation of the HIPAA Privacy Rule); (b) your PHI has not been encrypted to government standards; and (c) my risk assessment fails to determine that there is a low probability that your PHI has been compromised.

- For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html

BREACH NOTIFICATION ADDENDUM

The incorporation of the Health Information Technology for Economic and Clinical Health (HITECH) Act added a requirement to HIPAA that counselors (and other covered entities) must give notice to clients/patients and to the U.S. Department of Health and Human Services (HHS) if they discover that “unsecured” Protected Health Information (PHI) has been breached. A “breach” is defined as the acquisition, access, use or disclosure of PHI in violation of the HIPAA Privacy Rule.

- Examples of a breach include: stolen or improperly accessed PHI; PHI inadvertently sent to the wrong provider; and unauthorized viewing of PHI by a practice employee. PHI is “unsecured” if it is not encrypted to government standards.

Use or disclosure of PHI that violates the Privacy Rule is presumed to be a breach unless a provider demonstrates that there is a “low probability that PHI has been compromised.”

1. When a practice becomes aware of or suspects a breach, the practice will conduct a Risk Assessment and keep a written record of that Risk Assessment. The risk assessment considers the following four factors to determine if PHI has been compromised:

- The nature and extent of PHI involved (e.g., whether the breached PHI provides client/patient names, or other information enabling an unauthorized user to determine the client’s/patient’s identity)
- To whom the PHI may have been disclosed. This refers to the unauthorized person who used the PHI or to whom the disclosure was made. That person could be an outside thief or hacker, or a knowledgeable insider who inappropriately accessed client/patient records.
- Whether the PHI was actually acquired or viewed.
- The extent to which the risk to the PHI has been mitigated. For example, if the wrong client’s/patient’s PHI is sent to a psychologist colleague for consultation, a provider can obtain written confirmation from the colleague that they will properly delete or destroy the PHI on the wrong client/patient. By contrast, if a laptop has been stolen there is little assurance that the thief will respect a client’s/patient’s confidentiality.

2. Unless the practice determines that there is a low probability that PHI has been compromised, the practice will give notice of the breach. If notice is required, providers must notify any client/patient affected by a breach without unreasonable delay and within 60 days after discovery. A breach is “discovered” on the first day that a provider knows (or reasonably should have known) of the breach. The notice must be in plain language that a client/patient can understand and should provide brief description of the breach, including dates; a description of types of unsecured PHI involved; the steps the client/patient should take to protect against potential harm; a brief description of steps that the practice has taken to investigate the incident, mitigate harm, and protect against further breaches; and provider contact information. Written notice must be provided by first class mail to the client/patient at his or her last known address or contact may be made via e-mail if a client/patient has indicated that this is their preferred mode of contact. For breaches affecting fewer than 500 patients, the provider must keep a log of those breaches during the year and then provide notice to HHS of all breaches during the calendar year, within 60 days after that year ends.

3. The risk assessment can be done by a business associate if it was involved in the breach. While the business associate will conduct a risk assessment of a breach of PHI in its control, the practice will provide any required notice to clients/patients and HHS.

4. After any breach, particularly one that requires notice, the practice will re-assess its privacy and security practices to determine what changes should be made to prevent the re-occurrence of such breaches.

QUESTIONS AND COMPLAINTS

- If you have questions or need further assistance regarding this notice, you may contact Lindsay Martin, PhD, LPC, NCC by email at lindsay@drlindsaymartin.com.
- If you believe your privacy rights have been violated, you may file a complaint in writing to Lindsay Martin, PhD, LPC, NCC by email at lindsay@drlindsaymartin.com.
- You may also file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201.
- Additional information is available by visiting www.hhs.gov/ocr/privacy/hipaa/complaints/ or by calling 1-877-696-6775.
- All complaints must be made in writing and will in no way affect the quality of care you receive from me.

EFFECTIVE DATE OF THIS NOTICE

The Health Insurance Portability and Accountability Act (HIPAA) privacy regulations went into effect on April 14, 2003. Compliance requirements with final modifications to the HIPAA privacy and security rule went into effect on September 23, 2013.

By signing below, I acknowledge that I have received a copy of the Notice of Counselors’ Policies and Practices to Protect the Privacy of Your Health Information.

Client or Parent/Guardian Print Name: _____

Signature of Client or Parent/Guardian

Date

Therapist Print Name: _____

Signature of Therapist

Date