WHICHARD
psychological services PLLC

S. Michelle Whichard, PhD.
Licensed Psychologist (LP)
Health Service Provider-Psychologist (HSP-P)
Nationally Certified School Psychologist (NCSP)

1829 E. Franklin Street, Building #900A, Chapel Hill, NC 27514
michelle@whichardps.com
www.whichardps.com
(919) 623-1448; (919) 869-2814 (fax)

Notice of Privacy Practices for Protected Health Information

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY!

I am permitted by federal privacy laws to make uses and disclosures of your health information for purposes of treatment, payment, and health care operations with your consent.

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

- *"Protected health information (PHI)"* is the information in your health record that could identify you. Such information may include medical history, assessment information, and billing documents.
- *An Example of "Using of Your Health Information for Treatment" would be when* I consult with another health care provider who is working with you, such as your family physician.
- *An Example of "Using of Your Health Information for Payment" would be when* I disclose your PHI to your insurer to obtain reimbursement for your healthcare or to determine eligibility or coverage.
- *Examples of "Health Care Operations" include* activities related to the performance and operation of my practice such as quality assessment and improvement activities, audits, and case management and care coordination.
- *"Use"* applies only to activities within this practice such as sharing, employing, applying, utilizing, examining, and analyzing information that identifies you.
- *"Disclosure"* applies to activities outside of this practice group, such as releasing, transferring, or providing access to information about you to other parties.

Also included in this type of disclosure is when I contact you to arrange an appointment.

II. Uses and Disclosures Requiring Authorization

I may use or disclose your PHI for purposes outside of treatment, payment, and healthcare operations when your authorization is obtained. An authorization is written permission above and beyond the general consent form that permits only specific disclosures. When I am asked for information for purposes outside of treatment, payment, and healthcare operations I will obtain authorization from you before releasing this information. "*Psychotherapy noes"*

are kept separate from your medical record. These are notes made by your doctor about your conversation during a private, group, joint, or family counseling session, and are given a greater degree of protection than your general record. They cannot be released on a general Authorization request for your medical record.

You may revoke all such authorizations at any time, provided each revocation is in writing. You may not revoke an authorization (1) after information has been released or (2) if the authorization was obtained as a condition of obtaining insurance coverage, and the law provides the insurer the right to contest the claim under the policy.

I will also obtain an authorization from you before using or disclosing PHI in a way that is not described in this Notice.

III. Disclosures and Uses without Consent or Authorization

I may disclose your PHI without your consent under the following circumstances:

- **Abuse & Neglect**
  I may disclose your protected health information to public authorities such as the County Department of Social Services as mandated by law to report abuse or neglect of a child or disabled adult. If asked by the Director of Social Services to turn over information from your records relevant to a child protective services investigation, I must do so.

- **Health Oversight**
  Government and other agencies have the right to request information as part of health oversight activities. For example, the North Carolina Psychology Board has the power to subpoena relevant records should I be the focus of inquiry.

- **Judicial/Administrative Proceedings**
  I may disclose your protected health information in the course of any judicial or administrative proceeding as directed by a proper court order. If you are involved in a court proceeding, and a request is made for information about the professional services provided to you and/or records thereof, such information is privileged under state law, and must not be released without your written authorization or court order. This 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.

- **Serious Threat**
  I may disclose your protected health information to protect you or others from a serious threat of harm by you.

- **Worker's Compensation**
  If you file a worker's compensation claim, I am required by law to provide your mental health information relevant to the claim to both your employer and to the North Carolina Industrial Commission.

When the use and disclosure without your consent or authorization is allowed under other sections of Section 164.512 of the Privacy Rule and the state's confidentiality law. This includes certain narrowly-defined disclosures to law enforcement agencies, to a health oversight agency (such as HHS or a state department of health), to a coroner or medical examiner, for public health purposes relating to disease or FDA-regulated products, or for specialized government functions such as fitness for military duties, eligibility for VA benefits, and national security and intelligence.

IV. Your Health Information Rights

You have a right to:

- ***Request a restriction*** on certain uses and disclosures of your health information. While I make every effort to honor your request, I am not required to grant the request.
- ***Obtain a paper copy*** of the current Notice of Privacy Practices for Protected Health Information.
- ***Request that you be allowed to inspect and copy*** your health record and billing record – you may exercise this right by delivering the request to my office.
- ***Appeal a denial of access*** to your protected health information.
- ***Request that your health care record be amended*** to correct incomplete or incorrect information. I may deny your request if you ask me to amend information 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 information that you would be permitted to inspect and copy; or
  - Is accurate and complete.

  If your request is denied, you will be informed of the reason for the denial and will have an opportunity to submit a statement of disagreement to be maintained with your records.

- Request that communication of your health information be made by alternative means or at an alternative location (for example, sending communication to you at another address).
- Obtain an accounting of disclosures of your health information for which you have provided neither consent nor authorization.
- Revoke authorizations that you made previously to use or disclose information by delivering a written revocation to my office, except to the extent information or action has already been taken.
- ***Restrict certain disclosures of PHI to a health plan when you pay out-of-pocket in full for my services***.
- ***Be Notified if There is a Breach of Your Unsecured PHI.*** For instance, if: (a) there is a breach (use or disclosure of your PHI in violation of the HIPAA Privacy Rule) involving your PHI; (b) that 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. *see attached Breach Notification attached.

If you want to exercise any of the above rights, please put your request in writing. I will inform you of the steps that need to be taken to exercise your rights.

V. Psychologist Responsibilities

I am required to:

- Maintain the privacy of your health information as required by law.
- Provide you with a notice as to my duties and privacy practices.
- Abide by the terms of this notice.
- Notify you if I cannot accommodate a requested restriction or request.
- Accommodate your reasonable requests regarding methods to communicate health information with you.

I have the right to amend, change, or eliminate provisions in these privacy practices and to enact new provisions regarding protected health information. If my information practices change, I will amend this Notice. You are entitled to receive a revised copy of the Notice by calling and requesting a copy or by visiting my office and picking up a copy.

VI. To Request Information or File a Complaint

If you have questions, would like additional information, or want to report a problem regarding the handling of your information, you may contact me in person or over the telephone at 919-623-1448.

Additionally, if you believe your privacy rights have been violated, you may file a written complaint with me. You may also file a complaint by mailing it or e-mailing it to the Secretary of Health and Human Services, whose street address and e-mail address is: Office for Civil Rights - U.S. Department of Health and Human Services - 200 Independence Avenue S.W. - Room 509F, HHH Building - Washington, D.C. 20201.

I cannot, and will not, require you to waive the right to file a complaint with the Secretary of Health and Human Services (HHS) as a condition of receiving treatment.

I cannot, and will not, retaliate against you for filing a complaint with the Secretary of Health and Human Services.

VII. Breach Notification Addendum to Policies & Procedures

- If I were to become aware of or suspect a breach (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 [e.g., laptop]; PHI inadvertently sent to the wrong provider; PHI is "unsecured" if it is not encrypted to government standards), then I would conduct a *Risk Assessment** as outlined by the U.S. Department of Health and Human Services (HHS), and I would keep a written record of that Risk Assessment.

- Unless I were to determine that there is a low probability that PHI has been compromised, I would give notice of the breach by giving notice to the patient and to HHS.

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

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

***** *Risk Assessment*

The risk assessment considers the following four factors to determine if PHI has been compromised:

- 1) **The nature and extent of PHI involved.** For example, does the breached PHI provide patient names, or other information enabling an unauthorized user to determine the patient's identity?
- 2) **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 patient records.
- 3) **Whether the PHI was actually acquired or viewed**. Factors 2 and 3 can be illustrated by comparing two scenarios. In both scenarios, my office has been broken into and the locked file cabinet with paper patient records has been pried open. In Scenario A, I may suspect that a burglar was simply looking for valuables because cash and other valuables (but no patient files) have been taken. In Scenario B, I may suspect the husband of a patient in the midst of a contentious divorce because no valuables have been taken; only the wife's file appears to have been opened, and the husband has a history of similar extreme behavior. In Scenario A, the likelihood that a burglar was rummaging through files seeking only valuables, indicates a relatively low risk that PHI was actually viewed. In Scenario B, the identity of the suspected "breacher" suggests a very high risk that the wife/patient's PHI was viewed and compromised.
- 4) **The extent to which the risk to the PHI has been mitigated**. For example, if I were to send the wrong patient's PHI to a psychologist colleague for consultation, it should be easy to obtain written confirmation from the colleague that they will properly delete or destroy the PHI on the wrong patient. By contrast, if my laptop

were to be stolen I would have little assurance that the thief will respect your confidentiality. If the risk assessment fails to demonstrate that there is a low probability that the PHI has been compromised, breach notification is required — **if** the PHI was unsecured.

VIII. Effective Date, Restrictions and Changes to Privacy Policy

This notice will go into effect September 23, 2013.

If material changes to privacy policies are made, copies of revised notices to active clients will be mailed. Copies of the most recent Notice may be obtained from Dr. Whichard by contacting 919-623-1448.