**Notice of Psychologists' Policies and Practices to Protect the Privacy of Your Health Information**

THIS 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.

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

I may *use* or *disclose* your *protected health information* (*PHI*), for *treatment, payment, and health care operations (TPO)* purposes with your *consent*. To help clarify these terms, here are some definitions:

- "*PHI"* refers to information in your health record that could identify you.
- *"Treatment, Payment and Health Care Operations"*
  – *Treatment* is when I provide, coordinate or manage your health care and other services related to your health care. An example of treatment would be when I consult with another health care provider, such as your family physician or another psychologist.
  - *Payment* is when I obtain reimbursement for your healthcare. Examples of payment are when I disclose your PHI to your health insurer to obtain reimbursement for your health care or to determine eligibility or coverage.
  - *Health Care Operations* are activities that relate to the performance and operation of my practice. Examples of health care operations are quality assessment and improvement activities, business-related matters such as audits and administrative services, and case management and care coordination.
- "*Use*" applies only to activities within my office such as sharing, employing, applying, utilizing, examining, and analyzing information that identifies you.
- "*Disclosure*" applies to activities outside of my office, such as releasing, transferring, or providing access to information about you to other parties.
- *"Consent"* is your agreement that I may use and/or disclose information about you and our work together. By signing the Acknowledgment of Receipt of this Notice, you give your consent for me to do so for purposes of treatment, payment, and health care operations.

II. Uses and Disclosures Requiring Authorization

I may use or disclose PHI for purposes outside of treatment, payment, and health care operations when your appropriate authorization is obtained. An "*authorization"* is written permission above and beyond the general consent that permits only specific disclosures.

In those instances when I am asked for information for purposes outside of treatment, payment and health care operations, I will obtain an authorization from you before releasing this information. I will also need to obtain an authorization before releasing your psychotherapy notes. *"Psychotherapy notes"* are notes I have made about our conversation during a private, group, joint, or family counseling session, which I have kept separate from the rest of your medical record. These notes are given a greater degree of protection than PHI.

You may revoke all such authorizations (of PHI or psychotherapy notes) at any time, provided each revocation is in writing. You may not revoke an authorization to the extent that (1) I have relied on that authorization; 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. Uses and Disclosures with Neither Consent nor Authorization

I may use or disclose PHI without your consent or authorization in the following circumstances:

- **Child Abuse:** If you give me information that leads me to suspect child abuse, neglect, or death due to maltreatment, I must report such information to the county Department of Social Services. If asked by the Department of Social Services to turn over information from your records relevant to a child protective services investigation, I must do so.

- **Adult and Domestic Abuse:** If information you give me gives me reasonable cause to believe that a disabled adult is in need of protective services, I must report this to the Department of Social Services.

- **Health Oversight:** The North Carolina Psychology Board has the power, when necessary, to subpoena relevant records should I be the focus of an inquiry.

- **Judicial or Administrative Proceedings:** If you are involved in a court proceeding, and a request is made for information about the professional services that I have provided you and/or the records thereof, such information is privileged under state law, and I must not release this information without your written authorization, or a 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 to Health or Safety:** I may disclose your confidential information to protect you or others from a serious threat of harm by you.

- **Worker's Compensation:** If you file a workers' compensation claim, I am required by law to provide your mental health information relevant to the claim to your employer and 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. Patient's Rights and Psychologist's Duties

Patient's Rights:

- *Right to Request Restrictions* –You have the right to request restrictions on certain uses and disclosures of protected health information about you. However, I am not required to agree to a restriction you request.

- *Right to Receive Confidential Communications by Alternative Means and at Alternative Locations* – You have the right to request and receive confidential communications of PHI by alternative means and at alternative locations. (For example, you may not want a family member to know that you are seeing me. Upon your request, I will send your bills to another address.)

- *Right to Inspect and Copy* – You have the right to inspect or obtain a copy (or both) of PHI in my mental health and billing records used to make decisions about you for as long as the PHI is maintained in the record. I may deny your access to PHI under certain circumstances, but in some cases, you may have this decision reviewed. On your request, I will discuss with you the details of the request and denial process.

- *Right to Amend* – You have the right to request an amendment of PHI for as long as the PHI is maintained in the record. I may deny your request. On your request, I will discuss with you the details of the amendment process.

- *Right to an Accounting* – You generally have the right to receive an accounting of disclosures of PHI for which you have neither provided consent nor authorization (as described in Section III of this Notice). On your request, I will discuss with you the details of the accounting process.

- *Right to a Paper Copy* – You have the right to obtain a paper copy of the notice from me upon request, even if you have agreed to receive the notice electronically

- *Right to Restrict Disclosures When You Have Paid for Your Care Out-of-Pocket* **-** 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 (a 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.

Psychologist's Duties:

- I am required by law to maintain the privacy of PHI and to provide you with a notice of my legal duties and privacy practices with respect to PHI (this document).
- I reserve the right to change the privacy policies and practices described in this notice. Unless I notify you of such changes, however, I am required to abide by the terms currently in effect.
- If I revise my policies and procedures, I will provide you with a copy at the next scheduled psychotherapy session.

I sometimes rely on certain persons or other entities, who or which are not my employees, to provide services on my behalf. These persons or entities may include accountants, lawyers, billing services, and collection agencies. Where these persons or entities perform services, which require the disclosure of individually identifiable health information, they are considered under the Privacy Rule to be my Business Associates.

I enter into a written agreement with each of my Business Associates to obtain satisfactory assurance that the Business Associate will safeguard the privacy of the PHI of my patients.

I rely on my Business Associate to abide by the contract but will take reasonable steps to remedy any breaches of the agreement that I become aware of.

V. Questions and Complaints

If you have questions about this notice, disagree with a decision I make about access to your records, or have other concerns about your privacy rights, you may contact me at this office.

If you believe that your privacy rights have been violated and wish to file a complaint with me, you may send your written complaint to me at 104 So. Estes Drive, Suite 206, Chapel Hill, NC 27514.

You may also send a written complaint to the Secretary of the U.S. Department of Health and Human Services. That address is: The Honorable Secretary of Health and Human Services, The U.S. Department of Health and Human Services, 200 Independence Avenue, S.W., Washington, D.C. 20201

You have specific rights under the Privacy Rule. I will not retaliate against you for exercising your right to file a complaint.

VI. Effective Date, Restrictions and Changes to Privacy Policy

This notice will go into effect on September 23, 2013.

**Breach Notification Addendum to Policies & Procedures**

When I become aware of or suspect a breach, as defined in Section 1 of the breach notification (below), I will conduct a Risk Assessment, as outlined in Section 2.A. I will keep a written record of that Risk Assessment.

Unless I determine that there is a low probability that PHI has been compromised, I will give notice of the breach as described in Sections 2.B and 2.C of the breach notification (below).

The risk assessment can be done by a Business Associate if he/she was involved in the breach. While the Business Associate will conduct a risk assessment of a breach of PHI in his/her control, I will provide any required notice to patients and HHS.

After any breach, particularly one that requires notice, I will re-assess my privacy and security practices to determine what changes should be made to prevent the re-

occurrence of such breaches.

**BREACH NOTIFICATION** ***(The language in this section is directed at psychologists; I include it here so that patients can see the extent to which I will strive to protect them in the event of a breach.)***

**1. What is a Breach?** The HITECH Act added a requirement to HIPAA that psychologists (and other covered entities) must give notice to patients and to 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 tothe wrong provider; and unauthorized viewing of PHI by an employee in your practice. PHI is "unsecured" if it is not encrypted to government standards. A use or disclosure of PHI that violates the Privacy Rule is *presumed* to be a breach unless you demonstrate that there is a "low probability that PHI has been compromised." That demonstration is done through the risk assessment described next.

**2. What to Do if You Learn of or Suspect a Breach**

**A. Risk Assessment**

The first step if you discover or suspect a breach is to conduct the required risk assessment. (You must take this step even if the breached PHI was secured through encryption.) 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, your office has been broken into and your locked file cabinet with paper patient records has been pried open. In Scenario A, you suspect that a burglar was simply looking for valuables because cash and other valuables (but no patient files) have been taken. In Scenario B, you suspect the husband of a patient inthe 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 you 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 your laptop has been stolen you have little assurance that the thief will respect your patient's 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.

***Important Tip: Encryption*** *– This is a powerful incentive touse increasingly affordable encryption technology. If you suffer a breach and the PHI is properly encrypted, you are spared the trouble and embarrassment of giving breach notification. More importantly, your patient's privacy is protected because it is very difficult for the breacher to crack your encryption.*

Regardless of whether you determine that notice is required, you should document your risk assessment of all potential breaches. We also recommend that you reassess your practice's privacy and security practices/procedures after any breach to prevent the same lapse from reoccurring.

**B. Notice to the Patient**

If notice is required, you must notify any patient affectedby a breach without unreasonable delay and within 60 days after discovery. A breach is "discovered" on the first day that you know (or reasonably should have known) of the breach. You are also deemed to have discovered a breach on the first day that any employee, officer or other agent of your practice (other than the person who committed the breach) knows about the breach.

In most cases that members have brought to the APA Practice Organization's attention, there is a clear answer to the question, "Do I have to give notice?" For example, in the most common scenario of the stolen laptop with unencrypted PHI, the answer is always yes. But if you are uncertain, you can contact our Office of Legal and Regulatory Affairs at praclegal@apa.org. You may also want to contact your professional liability insurance.

The notice must be in plain language that a patient can understand. It should provide:

· A brief description of the breach, including dates

· A description of types of unsecured PHI involved

· The steps the patient should take to protect against potential harm

· A brief description of steps you have taken to investigate the incident, mitigate harm, and protect against further breaches; and

· Your contact information.

If you do not have all of the above information when you first need to send notice, you can provide a series of notices that fill in the information as you learn it. You must provide written notice by first-class mail to the patient at his or her last known address. Alternatively, you can contact your patients by e-mail if they have indicated that this is the preferred mode of contact.

**C. Notice to HHS**

For breaches affecting fewer than 500 patients, you 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. For breaches affecting 500 patients or more, there are more complicated requirements that include immediate notice to HHS and sending notifications to major media outlets in the area for publication purposes. HHS provides instructions on how to provide notice for breaches affecting more than 500 patients on its website at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.