Eugene Kranz, Ph.D. CA PSY Lic #: 23155

NOTICE OF PRIVACY PRACTICES

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.

Privacy is a very important concern for all those who come to this office. It is also complicated because of the many federal and state laws and our professional ethics. Because the rules are so complicated, some parts of this notice are very detailed, and you probably will have to read them several times to understand them. If you have any questions, please do not hesitate to ask. We will discuss this form in detail during our first meeting and I would be happy to answer any of your questions then, or when they arise.

Contents of this notice

A. Introduction: To my patients

This notice will tell you how I handle your medical information. It tells how I use this information here in this office, how I share it with other professionals and organizations, and how you can see it. I want you to know all of this so that you can make the best decisions for yourself and your family. If you have any questions or want to know more about anything in this notice, please ask for more explanations or more details.

B. What I mean by your medical information

Each time you visit me or any doctor's office, hospital, clinic, or other health care provider, information is collected about you and your physical and mental health. It may be information about your past, present, or future health or conditions, or the tests and treatment you received from me or from others, or about payment for health care. The information I collect from you is called **"PHI,"** which stands for **"protected health information."** This information goes into your **medical or health care records** in my office.

In this office, your PHI is likely to include these kinds of information:

- Your history: Things that happened to you as a child; your school and work experiences; your marriage and other personal history.
- Reasons you came for treatment: Your problems, complaints, symptoms, or needs.
- Diagnoses: These are the medical terms for your problems or symptoms.
- A treatment plan: This is a list of the treatments and other services that I think will best help you.

- Progress notes: Each time you come in, I write down some things about how you are doing, what I notice about you, and what you tell me.
- Records I get from others who treated you or evaluated you.
- Psychological test scores, school records, and other reports.
- Information about medications you took or are taking.
- Legal matters.
- Billing and insurance information.

There may also be other kinds of information that go into your health care records here.

I may use PHI for many purposes. For example, I may use it:

- To plan your care and treatment.
- To decide how well my treatments are working for you.
- When I talk with other health care professionals who are also treating you, such as your family doctor or the professional who referred you to me.
- To show that you actually received services from me, which I billed to you or to your health insurance company.
- For teaching and training other health care professionals.
- For medical or psychological research.
- For public health officials trying to improve health care in this area of the country.
- To improve the way I do my job by measuring the results of my work.

When you understand what is in your record and what it is used for, you can make better decisions about who, when, and why others should have this information.

C. Privacy and the laws about privacy

I am required to tell you about privacy because of a federal law, the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA requires me to keep your PHI private and to give you this notice about my legal duties and my privacy practices. I will obey the rules described in this notice. If I change my privacy practices, they will apply to all the PHI I keep. I will also post the new notice of privacy practices in my office where everyone can see. You or anyone else can also get a copy about my privacy policy by asking me or by finding it on my website at: www.drgenekranz.com or www.thebodymindsolution.com .

D. Breach notification

When I become aware of or suspect a breach, as defined in Section 1 of the breach notification overview, I will conduct a Risk Assessment, as outlined in Section 2.A of the Overview. 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 Overview. 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 **(see Attachment I for more details).

E. How your protected health information can be used and shared

Except in some special circumstances, when I use your PHI in this office or disclose it to others, I share only the **minimum necessary** PHI needed for those other people to do their jobs. The law gives you rights to know about your PHI, to know how it is used, and to have a say in how it is shared. So I will tell you more about what I do with

your information. Mainly, I will use and disclose your PHI for routine purposes to provide for your care, many of which do not require prior written consent or authorization. For other uses, I must tell you about them and ask you to sign a written authorization form.

1. Uses and disclosures that DO NOT require your prior written consent or authorization

In almost all cases I intend to use your PHI here or share it with other people or organizations to provide treatment to you, arrange for payment for my services, or some other business functions called "health care operations." In other words, I need information about you and your condition to provide care to you.

a. The basic uses and disclosure that DO NOT require prior written consent or authorization

For treatment. I use your medical information to provide you with psychological treatments or services. These might include individual, family, or group therapy; psychological, educational, or vocational testing; treatment planning; or measuring the benefits of my services.

I may share your PHI with others who provide treatment to you. For example, I may share your information with your personal physician or psychiatrist. If you are being treated by a team, I can share some of your PHI with the team members, so that the services you receive will work best together. The other professionals treating you will also enter their findings, the actions they took, and their plans into your medical record, and so we all can decide what treatments work best for you and make up a treatment plan. I may refer you to other professionals or consultants for services I cannot provide. When I do this, I need to tell them things about you and your conditions. I will get back their findings and opinions, and those will go into your records here. If you receive treatment in the future from other professionals, I can also share your PHI with them. These are some examples so that you can see how I use and disclose your PHI for treatment.

For payment. I may use your information to bill you, your insurance, or others, so I can be paid for the treatments I provide to you. I may contact your insurance company to find out exactly what your insurance covers. I may have to tell them about your diagnoses, what treatments you have received, and the changes I expect in your conditions. I will need to tell them about when we met, your progress, and other similar things.

For health care operations. Using or disclosing your PHI for health care operations goes beyond our care and your payment. For example, I may use your PHI to see where I can make improvements in the care and services I provide. I may be required to supply some information to some government health agencies, so they can study disorders and treatment and make plans for services that are needed. If I do, your name and personal information will be removed from what I send.

Patient Incapacitation or Emergency. I may disclose your PHI to others without your consent if you are incapacitated or if an emergency exists. For example, your consent isn't required if you need emergency treatment, as long as I try to get your consent after treatment is rendered, of if I try to get your consent but you are unable to communicate with me (for example, if you are unconscious or in severe pain) and I think that you would consent to such treatment if you were able to do so.

b. Other uses and disclosures that also DO NOT require prior written consent or authorization

Legal mandates. When federal, state or local laws require disclosure. For example, I may have to make a disclosure to applicable governmental officials when a law requires me to report information to government agencies and law enforcement personnel about victims of abuse or neglect. I have to report suspected child abuse, elder and/or dependent adult abuse.

Safety concerns. Disclosure of your PHI may be required to avert a serious threat to health or safety. For example, I may have to use or disclose your PHI to avert a serious threat to the health or safety of yourself or

to the health and safety of other(s). Any such disclosure will only be made to someone able to prevent the threatened harm from occurring.

Judicial or legal proceedings. When judicial or administrative proceedings require disclosure. For example, if you are involved in a lawsuit or a claim for worker's compensation benefits, I may have to use or disclose your PHI in response to a court or administrative order. I may also have to use or disclose your PHI in response to a subpoena. I am legally obligated to respond to the subpoena and may have to provide the requested information to the court. However, such information is also likely to be privileged under CA law, and I will not release information without first consulting with you or your legally appointed representative. This does not apply when you are being evaluated by a third party or where the evaluation is court ordered. You will be informed in advance if this is the case.

Law enforcement. When law enforcement requires disclosure. For example, I may have to use or disclose your PHI in response to a search warrant.

Health oversight. When public health activities require disclosure. For example, I may have to use or disclose your PHI to report to a government official an adverse reaction that you have to a medication. I may have to provide information to assist the government in conducting an investigation or inspection of a health care provider or organization. I also have to disclose some information to the government agencies that check on us to see that I am obeying privacy laws (e.g. Quality Care Reviews).

Government functions. If you are in the military, I may have to use or disclose your PHI for national security purposes, including protecting the President of the United States or conducting intelligence operations.

Appointment reminders. I may use and disclose your PHI to reschedule or remind you of appointments for treatment or other care. If you want me to call or write to you only at your home or your work, or you prefer some other way to reach you, I usually can arrange that. Just tell me.

Treatment alternatives and/or benefits. I may use and disclose your PHI to tell you about or recommend possible treatments or alternatives that may be of help to you, or other health care benefits that I offer that may be of interest to you.

Research. I may use or share your PHI to do research to improve treatments—for example, comparing two treatments for the same disorder, to see which works better or faster or costs less. In all cases, your name, address, and other personal information will be removed from the information given to researchers. If they need to know who you are, I will discuss the research project with you, and I will not send any information unless you sign a special authorization form.

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.

2. Uses and disclosures that require your authorization

If I want to use your information for any purpose besides those described above, I need your written permission on an authorization form. I don't expect to need this very often. If you do allow me to use or disclose your PHI, you can cancel that permission in writing at any time. I would then stop using or disclosing your information for that purpose. Of course, I cannot take back any information I have already disclosed or used with your permission. I will obtain an authorization from you before using or disclosing PHI in a way that is not described in this Notice.

3. Uses and disclosures where you have an opportunity to object

I may provide some information about you with your family or close others who you indicate is involved in your care or the payment for your heath care, unless you object in whole or in part. I will ask you which persons you want me to tell, and what information you want me to tell them, about your condition or treatment, as long as it is not against the law.

4. An accounting of disclosures I have made. When I disclose your PHI, I may keep some records of whom I sent it to, when I sent it, and what I sent. You can get an accounting (a list) of these disclosures.

F. Your rights concerning your health information

1. Right to Receive Communication by Alternative Means or at Alternative Locations. You can ask me to communicate with you about your health and related issues in a particular way or at a certain place that is more private for you. For example, you can ask me to call you at home, and not at work, to schedule or cancel an appointment.

2. Right to Request Restrictions. You have the right to ask me to limit what I tell people involved in your care or with payment for your care, such as family members and friends. I don't have to agree to your request, but if we do agree, I will honor it except when it is against the law, or in an emergency, or when the information is necessary to treat you.

3. Right to Inspect and Copy. In most cases, you have the right to look at the health information I have about you, such as your medical and billing records. You must make the request to inspect or copy such information in writing. You can get a copy of these records, but I may charge you. I will respond to your request within 30 days of receiving your written request. In certain situations, I may deny your request. If I do, I will tell you, in writing, my reasons for the denial and explain your right to have my denial reviewed. I may provide you with a summary of your PHI as long as you agree to that in advance.

4. Right to Amendment. If you believe that the information in your records is incorrect or missing something important, you can ask me to make additions to your records to correct the situation. You have to make this request in writing and send it to me. You must also tell me the reasons you want to make the changes.

5. Right to Privacy Policy. You have the right to a copy of this notice. If I change this notice, I will post the new one in my office or you can find it on my website.

6. You have the right to file a complaint if you believe your privacy rights have been violated. You can file a complaint with me, Eugene Kranz, Ph.D. and/or with the Secretary of the U.S. Department of Health and Human Services. All complaints must be in writing. Filing a complaint will not change the health care I provide to you in any way.

7. Right to Accounting. You generally have a right to receive an accounting of disclosure of your PHI. Upon your request, I will discuss with you the details of this accounting process.

8. Right to Restrict for Care Out-of-Pocket. You have the right to restrict certain disclosure of PHI to a health plan when you pay out-of-pocket in full for my services.

9. Right to be Notified. You have a right to be notified if: a). there is a breach (a use or disclosure of your PHI in violation of the HIPPAA 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.

You may have other rights that are granted to you by the laws of our state, and these may be the same as or different from the rights described above. I will be happy to discuss these situations with you now or as they arise.

F. If you have questions or problems

If you need more information, have questions about the privacy practices described above, or have other concerns about your privacy rights, you may contact me, Eugene Kranz, Phs.D. at 805-748-3055 or via email at drgenekranz@gmail.com.

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: Eugene Kranz, Ph.D., P.O. Box 13125, San Luis Obispo, CA 93406. You may also send a written complaint to the Secretary of the U.S. Department of Health and Human Services. I can provide you with appropriate address upon request. Please note: you have specific rights under the Privacy Rule. I will not retaliate against you for exercising your right to file a compliant.

The effective date of this revised notice went into effect on revised effective September 23, 2013.

Attachment I: Breach Notification

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 to the 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.

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 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 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.

B. Notice to the Patient

If notice is required, you must notify any patient affected by 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

Attachment I: Breach Notification (cont).

· 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.