CONSENT FOR THE PURPOSES OF TREATMENT, PAYMENT AND HEALTHCARE OPERATIONS

I consent to the use or disclosure of my protected health information by Betty Devers, Ed.D. for the purpose of diagnosing or providing treatment to me, obtaining payment for my health care bills, or to conduct health care operations. I understand that diagnosis and/or treatment of me by Dr. Devers may be conditioned upon my consent as evidenced by my signature on this document.

My "protected health information" means health information, including demographic information, collected from me and created or received by my psychologist, another health care provider, a health plan, my employer, or a health care clearinghouse. This protected health information relates to my past, present, or future physical or mental health or condition and identifies me, or there is a reasonable basis to believe the information may identify me.

I understand I have the right to request a restriction as to how my protected health information is used or disclosed to carry out treatment, payment, or health care operations. Dr. Devers is not required to agree to the restrictions that I may request. However, if Dr. Devers agrees to a restriction that I request, the restriction is binding on Dr. Devers.

I understand that I have the right to restrict certain disclosures of my protected health information to a health plan when I pay out-of-pocket in full for my services. I understand that I have the right to be notified if (a) there is a breach (a use or disclosure of my protected health information in violation of the HIPAA Privacy Rule); (b) my protected health information has not been encrypted to government standards; and (c) Dr. Devers' risk assessment fails to determine that there is a low probability that my protected health information has been compromised.

I have the right to revoke this consent, in writing at any time, except to the extent that Dr. Devers has taken action in reliance on this consent.

I understand I have a right to review Dr. Devers' Notice of Privacy Practices prior to signing this document as it has been provided to me. The Notice of Privacy Practices describes the types of uses and disclosure of my protected health information that will occur in my treatment, payment of my bills, or in the performance of health care operations of Dr. Devers. This notice of Privacy Practices also describes my rights and Dr. Devers' duties with respect to my protected health information. The Notice of Privacy Practices is provided in the office waiting room.

Dr. Devers reserves the right to change the privacy practices that are described in the Notice of Privacy Practices. I may obtain a revised notice of privacy practices by calling the office and requesting a revised copy to be sent in the mail or asking for one at the time of my next appointment.

BREACH NOTIFICATION ADDENDUM

1. When the practice becomes aware of or suspects a breach, as defined in the breach notification overview, the practice will conduct a Risk Assessment, as outlined in the overview. The practice will keep a written record of that Risk Assessment.
2. Unless the practice determines that there is a low probability that protected health information has been compromised, the practice will give notice of the breach as described in the breach notification overview.
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 protected health information in its control, the practice will provide any required notice to patients and the U.S. Department of Health and Human Services.
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.

Breach Notification Overview

HIPAA requires that psychologists (and other covered entities) must give notice to patients and to the U.S. Department of Human Health and Services if they discover that "unsecured" protected health information has been breached. A "breach" is defined as the acquisition, access, use, or disclosure of protected health information in violation of the HIPAA Privacy Rule. Examples of a breach include: stolen or improperly accessed private health information, private health information inadvertently sent to the wrong provider, and unauthorized viewing of private health information by an employee in the practice. Private health information is "unsecured" if it is not encrypted to government standards.

A use or disclosure of private health information that violates the Privacy Rule is presumed to be a breach unless the psychologist demonstrates that there is a "low probability that private health information has been compromised." That demonstration is done through the risk assessment.

Risk Assessment

If a breach is discovered or suspected, a risk assessment must be conducted. The risk assessment considers the following four factors to determine if private health information has been compromised:

1) The nature and extent of the private health information involved
2) To whom the private health information has been disclosed
3) Whether the private health information was actually acquired or viewed
4) The extent to which the risk to the private health information has been mitigated

If the risk assessment fails to demonstrate that there is a low probability that the private health information has been compromised, breach notification is required.

Regardless of whether it is determined that notice is required, the psychologist should document the risk assessment of all potential breaches. In addition, it is recommended that the psychologist reassess the practice's privacy and security practices/procedures after any breach to prevent the same lapse from reoccurring.

Notice to the Patient

If notice is required, the psychologist 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. The breach is also deemed to have been discovered on the first day that any employee, officer, or other agent of the practice (other than the person who committed the breach) knows about the breach.

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

1) A brief description of the breach, including dates
2) A description of types of unsecured private health information involved
3) The steps the patient should take to protect against potential harm
4) A brief description of steps that have been taken to investigate the incident, mitigate harm, and protect against further breaches, and
5) The psychologist's contact information

If the psychologist does not have all the above information when it is necessary to first send notice, they can provide a series of notices that fill in the information as they learn of it. Written notice must be provided by first-class mail to the patient at his/her last known address. Alternatively, contact can be made by email if the patient has indicated that this is the preferred mode of contact.

Notice to U.S. Department of Health and Human Services

For breaches affecting fewer than 500 patients, the psychologist must keep a log of those breaches during the year and then provide notice to the U.S. Department of Health and Human Services 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 the U. S. Department of Health and Human Services and sending notifications to major media outlets in the area for publication purposes.

Breaches Involving Business Associates

The risk assessment described above can be done by the psychologist's business associate if it was involved in the breach. A business associate is an organization or person outside the psychologist's practice to whom the psychologist sends or shares private health information so that they can provide services to you or on your behalf. Examples are: billing services, accountants, cloud storage, Health Information Organization (organizations that oversee the exchange of health related information), or collection agencies. Subcontractors who create, receive, maintain, or transmit private health information on behalf of the business associate are also included in the definition of business associate.

_____
Signature of Patient/Parent/Guardian

_____
Printed Name of Patient/Parent/Guardian

_____
Date