

Understanding How Your Privacy and Health Information is Protected

Dr. Skipper, LLC

125 Indiantown Road, Suite 203-A, Jupiter, Florida 33458
561-200-3381

Notice of Psychologists' Policies and Practices to Protect the Privacy of Your Health Information Effective Date: September 23, 2013

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.

We understand the importance of privacy and are committed to maintaining the confidentiality of your medical information. We make a record of the medical care we provide and may receive such records from others. We use these records to provide or enable other health care providers to provide quality medical care, to obtain payment for services provided to you as allowed by your health plan and to enable us to meet our professional and legal obligations to operate this medical practice properly. We are required by law to maintain the privacy of protected health information, to provide individuals with notice of our legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information. This notice describes how we may use and disclose your medical information. It also describes your rights and our legal obligations with respect to your medical information. If you have any questions about this Notice, please contact our Privacy Officer listed above.

Notice of Privacy Practices

This medical practice collects health information about you and stores it in a chart and on a computer. This is your medical record. The medical record is the property of this medical practice, but the information in the medical record belongs to you. The law permits us to use or disclose your health information for the following purposes:

1. Health Care Operations. We may share your medical information with our "business associates," such as our billing service, that perform administrative services for us. We have a written contract with each of these business associates that contains terms requiring them and their subcontractors to protect the confidentiality and security of your protected health information.
2. Appointment Reminders. We may use and disclose medical information to contact and remind you about appointments. If you are not home, we may leave this information on your answering machine or in a message left with the person answering the phone.
3. Notification and Communication with Family. We may disclose your health information to notify or assist in notifying a family member, your personal representative or another person responsible for your care about your location, your general condition or, unless you had instructed us otherwise, in the event of your death. In the event of a disaster, we may disclose information to a relief organization so that they may coordinate these notification efforts. We may also disclose information to someone who is involved with your care or helps pay for your care. If you are able and available to agree or object, we will give you the opportunity to object prior to making these disclosures, although we may disclose this information in a disaster even over your objection if we believe it is necessary to respond to the emergency circumstances. If you are unable or unavailable to agree or object, our health professionals will use their best judgment in communication with your family and others.
4. Required by Law. As required by law, we will use and disclose your health information, but we will limit our use or disclosure to the relevant requirements of the law. When the law requires us to report abuse, neglect or domestic violence, or respond to judicial or administrative proceedings, or to law enforcement officials, we will further comply with the requirement set forth below concerning those activities.
5. Public Health. We may, and are sometimes required by law, to disclose your health information to public health authorities for purposes related to: preventing or controlling disease, injury or disability; reporting child, elder or

dependent adult abuse or neglect; reporting domestic violence; reporting to the Food and Drug Administration problems with products and reactions to medications; and reporting disease or infection exposure. When we report suspected elder or dependent adult abuse or domestic violence, we will inform you or your personal representative promptly unless in our best professional judgment, we believe the notification would place you at risk of serious harm or would require informing a personal representative we believe is responsible for the abuse or harm.

6. Health Oversight Activities. We may, and are sometimes required by law, to disclose your health information to health oversight agencies during the course of audits, investigations, inspections, licensure and other proceedings, subject to the limitations imposed by law.
7. Judicial and Administrative Proceedings. We may, and are sometimes required by law, to disclose your health information in the course of any administrative or judicial proceeding to the extent expressly authorized by a court or administrative order. We may also disclose information about you in response to a subpoena, discovery request or other lawful process if reasonable efforts have been made to notify you of the request and you have not objected, or if your objections have been resolved by a court or administrative order.
8. Law Enforcement. We may, and are sometimes required by law, to disclose your health information to a law enforcement official for purposes such as identifying or locating a suspect, fugitive, material witness or missing person, complying with a court order, warrant, grand jury subpoena and other law enforcement purposes.
9. Public Safety. We may, and are sometimes required by law, to disclose your health information to appropriate persons in order to prevent or lessen a serious and imminent threat to the health or safety of a particular person or the general public.
10. Specialized Government Functions. We may disclose your health information for military or national security purposes or to correctional institutions or law enforcement officers that have you in their lawful custody.
11. Change of Ownership. In the event that this medical practice is sold or merged with another organization, your health information/record will become the property of the new owner, although you will maintain the right to request that copies of your health information be transferred to another physician or medical group.
12. Psychotherapy Notes. We will not use or disclose your psychotherapy notes without your prior written authorization except for the following: 1) use by the originator of the notes for your treatment, 2) for training our staff, students and other trainees, 3) to defend ourselves if you sue us or bring some other legal proceeding, 4) if the law requires us to disclose the information to you or the Secretary of HHS or for some other reason, 5) in response to health oversight activities concerning your psychotherapist, 6) to avert a serious and imminent threat to health or safety, or 7) to the coroner or medical examiner after you die. To the extent you revoke an authorization to use or disclose your psychotherapy notes, we will stop using or disclosing these notes.
13. Release of Information. An authorization for release of information must be signed before Dr. Skipper, LLC can release PHI for any uses and disclosures not described in this privacy notice. An authorization must also be signed for (A) most uses and disclosures of psychotherapy notes; (B) uses and disclosures of PHI for marketing purposes; (C) disclosures that constitute a sale of PHI.

When This Medical Practice May Not Use or Disclose Your Health Information

Except as described in this Notice of Privacy Practices, this medical practice will, consistent with its legal obligations, not use or disclose health information which identifies you without your written authorization. If you do authorize this medical practice to use or disclose your health information for another purpose, you may revoke your authorization in writing at any time.

Your Health Information Rights

1. Right to Request Special Privacy Protections. You have the right to request restrictions on certain uses and disclosures of your health information by a written request specifying what information you want to limit, and what limitations on our use or disclosure of that information you wish to have imposed. If you tell us not to disclose information to your commercial health plan concerning health care items or services for which you paid for in full out-of-pocket, we will abide by your request, unless we must disclose the information for treatment or legal reasons. We reserve the right to accept or reject any other request, and will notify you of our decision.
2. Right to Request Confidential Communications. You have the right to request that you receive your health information in a specific way or at a specific location. For example, you may ask that we send information to a particular e-mail account or to your work address. We will comply with all reasonable requests submitted in writing which specify how or where you wish to receive these communications.
3. Right to Inspect and Copy. You have the right to inspect and copy your health information, with limited exceptions. To access your medical information, you must submit a written request detailing what information you want access to, whether you want to inspect it or get a copy of it, and if you want a copy, your preferred form and format. We will provide copies in your requested form and format if it is readily producible, or we will provide you with an alternative format you find acceptable, or if we can't agree and we maintain the record in an electronic format, your choice of a readable electronic or hardcopy format. We will also send a copy to any other person you designate in writing. We will charge a reasonable fee which covers our costs for labor, supplies, postage, and if requested and agreed to in advance the cost of preparing an explanation or summary. We may deny your request under limited circumstances. If we deny your request to access your child's records or the records of an incapacitated adult you are representing because we believe allowing access would be reasonably likely to cause substantial harm to the patient, you will have a right to appeal our decision. If we deny your request to access your psychotherapy notes, you will have the right to have them transferred to another mental health professional.
4. Right to Amend or Supplement. You have a right to request that we amend your health information that you believe is incorrect or incomplete. You must make a request to amend in writing, and include the reasons you believe the information is inaccurate or incomplete. We are not required to change your health information, and will provide you with information about this medical practice's denial and how you can disagree with the denial. We may deny your request if we do not have the information, if we did not create the information (unless the person or entity that created the information is no longer available to make the amendment), if you would not be permitted to inspect or copy the information at issue, or if the information is accurate and complete as is. If we deny your request, you may submit a written statement of your disagreement with that decision, and we may, in turn, prepare a written rebuttal. All information related to any request to amend will be maintained and disclosed in conjunction with any subsequent disclosure of the disputed information.
5. Right to Restrict Certain Disclosures. You have the right to restrict certain disclosures of Protected Health Information (PHI) to a health plan if you pay out-of-pocket in full for the healthcare service.
6. 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.

If you would like to have a more detailed explanation of these rights or if you would like to exercise one or more of these rights, contact our Privacy Officer listed at the top of this Notice of Privacy Practices.

1. When Dr. Skipper, LLC becomes aware of or suspects a breach, as defined in section 1 of the breach notification Overview, Dr. Skipper, LLC will conduct a Risk Assessment, as outlined in Section 2.A of the Overview. Dr. Skipper, LLC will keep a written record of that Risk Assessment.
2. Unless Dr. Skipper, LLC determines that there is a low probability that PHI has been compromised, the practice will give notice of the breach as described in Sections 2.B and 2.C of the breach notification Overview.
3. The Risk Assessment can be done by a Business Associate if it was involved with the breach. While the business associate will conduct a Risk Assessment of a breach of PHI in its control, Dr. Skipper, LLC will provide any required notice to patients and HHS.
4. After any breach, particularly one that requires notice, Dr. Skipper, LLC 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

1. What is a Breach? The Health Information Technology for Economic and Clinical Health (HITECH) Act added a requirement to HIPAA that psychologists (and other covered entities) must give notice to 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 an employee at Dr. Skipper, LLC. 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 Dr. Skipper, LLC demonstrates 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 Dr. Skipper, LLC learns of or Suspects a Breach

A. Risk Assessment This first step is a breach is suspected is to conduct the required risk assessment. This step must be taken even if 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; (2) To whom the PHI may have been disclosed; (3) Whether the PHI was actually acquired or viewed; (4) The extent to which the risk to the PHI has been mitigated.

B. Notice to the Patient/Client If notice is required, Dr. Skipper, LLC 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 Dr. Skipper, LLC knows (or reasonable should have known) of the breach. Dr. Skipper, LLC is also deemed to have discovered a breach 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 must be in plain language that a patient can understand and should provide (1) a brief description of the breach, including dates; (2) a description of types of unsecured PHI involved; (3) The steps the patient should take to protect against potential harm; (4) A brief description of steps Dr. Skipper, LLC has taken to investigate the incident, mitigate harm, and protect against further breaches; (5) and Dr. Skipper, LLC contact information. If all of the previous information is not known at the first need to send notice, a series of notices that fill in the information as learned can be sent. Dr. Skipper, LLC must provide written notice by first-class mail to the patient at his or her last known address. Alternatively, patients can be contacted 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, a log must be kept of the 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.

3. Breaches Involving Business Associates The Final Rule clarified the role of business associates in breach notification. The risk assessment described in 2.A can be done by the business associate if it was involved in the breach.

Changes to this Notice of Privacy Practices

We reserve the right to amend this Notice of Privacy Practices at any time in the future. Until such amendment is made, we are required by law to comply with the terms of this Notice currently in effect. After an amendment is made, the revised Notice of Privacy Protections will apply to all protected health information that we maintain, regardless of when it was created or received. We will keep a copy of the current notice posted in our reception area, and a copy will be available at each appointment. We will also post the current notice on our website at www.drskipper.com.

Complaints

Complaints about this Notice of Privacy Practices or how this medical practice handles your health information should be directed to our Privacy Officer listed at the top of this Notice of Privacy Practices.

If you are not satisfied with the manner in which this office handles a complaint, you may submit a formal complaint to:

OCRMail@hhs.gov

The complaint form may be found at www.hhs.gov/ocr/privacy/hipaa/complaints/hipcomplaint.pdf. You will not be penalized in any way for filing a complaint.

