Health Insurance Portability and Accountability Act (HIPPAA)
PRIVACY POLICIES & PROCEDURES

Use and Disclosure of Protected Health Information (PHI): Protected Health Information ("PHI") may not be used or disclosed in violation of the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule (45 C.F.R. parts 160 and 164) (hereinafter, the "Privacy Rule") or in violation of state law.
I am permitted, but not mandated, under the Privacy Rule to use and disclose PHI without patient consent or authorization in limited circumstances. However, state or federal law may supercede, limit, or prohibit these uses and disclosures. Under the Privacy Rule, these permitted uses and disclosures include those made:

- To the patient
- For treatment, payment, or health care operations purposes, or
- As authorized by the patient.

Additional permitted uses and disclosures include those related to or made pursuant to:

- Reporting on victims of child or elder abuse, as required by law
- Court orders
- Workers' compensation laws
- Serious threats to health or safety
- Notifying the Department of Human Services in compliance with the FOID Mental Health Reporting Requirements
- 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.

I do not use or disclose PHI in ways that would be in violation of the Privacy Rule or state law. I use and disclose PHI as permitted by the Privacy Rule and in accordance with state or other law. In using or disclosing PHI, I meet the Privacy Rule's "minimum necessary requirement," as appropriate.

Use and Disclosure of PHI—Minimum Necessary Requirement: When using, disclosing or requesting PHI, I make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. I recognize that the requirement also applies to covered entities that request my patients' records and require that such entities meet the standard, as required by law. The minimum necessary requirement does not apply to disclosures for treatment purposes or when I share information with a patient. The requirement does not apply for uses and disclosures when patient authorization is given. It does not apply for uses and disclosures as required by law or to uses and disclosures that are required for compliance with the Privacy Rule.

Disclosures - If I receive a request for a non-routine disclosure of PHI that is not accompanied by a signed Authorization to Release Confidential Information, I am will not release the information or confirm that the individual is a client, until an Authorization is signed. It is my policy to notify you of any such requests I receive. In the event of non-routine disclosure of PHI, I will discuss my intention to disclose PHI before I do so, unless it is not possible. In the event it is not possible, I will discuss the disclosure with you as soon after it has occurred as possible. I keep records of all disclosures of PHI, including when to whom and what information was provided.
Consultation - I often consult with colleagues regarding clinical issues. When doing so, I will not reveal identifying information. The consultant will also be legally bound to keep this information private.

I will not use, disclose, or request an entire medical record, except when the entire medical record is justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

Use and Disclosure of PHI—Psychotherapy Notes Authorization: In some situations, I may opt to keep separate psychotherapy notes. I abide by the Psychotherapy Notes authorization requirement of the Privacy Rule, unless otherwise required by law. In addition, authorization is not required in the following circumstances--

- For my use for treatment
- To defend myself in a legal action brought by the patient, who is the subject of the PHI
- For purposes of HHS in determining my compliance with the Privacy Rule
- By a health oversight agency for a lawful purpose related to oversight of my practice
- To a coroner or medical examiner
- In instances related to a serious or imminent threat to the health or safety of a person or the public.

I recognize that a patient may revoke an authorization at any time in writing, except to the extent that I have, or another entity has, taken action in reliance on the authorization. Psychotherapy Notes are kept in an electronic file separate from other PHI. With exceptions for the aforementioned situations, in order for psychotherapy notes, or their contents to be released, the client (or guardian) must sign a valid authorization form. I will document and retain such authorization. If an outside party requests psychotherapy notes, or their contents, they

must provide a copy of a valid authorization form. I will also obtain an authorization from you before using or disclosing PHI in a way that is not described in this Notice.

Patient Rights—Notice: As required under the Privacy Rule, and in accordance with state law, I provide notice to patients of the uses and disclosures that may be made regarding their PHI and my duties and patient rights with respect to notice. I make a good faith effort to obtain written acknowledgment that my patient receives this notice. I provide notice to my patient on the first date of treatment and obtain from a patient (or guardian) written acknowledgement of receipt of the notice. I promptly revise and distribute notice whenever there is a material change to uses and disclosures, patient's rights, my legal duties, or other privacy practices stated in the notice.

Patient Rights—Restrictions and Confidential Communications: If you would like to restrict access to your PHI, you may submit your request to me in writing. I am not required to accommodate requests to restrict the use and disclosure of information, but once agreed upon, I may not violate the agreement. Restricted PHI may be provided to another health care provider in an emergency treatment situation. A restriction is not effective to prevent uses and disclosures when a patient requests access to his or her records or requests an accounting of disclosures. A restriction is not effective for any uses and disclosures authorized by the patient, or for any required or permitted uses recognized by law. Termination of the restriction may be submitted orally or in writing and I will document such termination. I permit patients *to request* receiving communications through alternative means or at alternative locations and I accommodate reasonable requests. I may not require an explanation for a confidential communication request, and reasonable accommodation may be conditioned on information on how payment will be handled and specification of an alternative address or method of contact.

Patient Rights—Access to and Amendment of Records: In accordance with state law, the Privacy Rule, and other federal law, patients have access to and may obtain a copy of the medical and billing records that I maintain. Patients are also permitted to amend their records in accordance with such law.

Patient Rights—Accounting of Disclosures: I provide my patients with an accounting of disclosures upon request, for disclosures made up to six years prior to the date of the request. While I may, I do not have to provide an accounting for disclosures made for treatment, payment, or health care operations purposes, or pursuant to patient authorization. Patients may request an account of disclosures by submitting a request in writing. The request must state the time period for which the accounting is to be supplied, which may not be longer than six years. The request must state whether the patient wishes to be sent the accounting via postal or electronic mail. For each disclosure in the accounting--the date, name and address (if known) of the entity that received the PHI, a brief description of the PHI disclosed, and a brief statement of the purpose of the disclosure that reasonably informs the patient of the basis of the disclosure—is provided. I provide an accounting within 60 days of a request, and that I may extend this limit for up to 30 more days by providing the patient with a written statement of the reasons for the delay and the date that the accounting will be provided. The first accounting is provided without charge. For each subsequent request I may charge a reasonable, cost-based fee. I will inform the patient of this fee and provide the patient the option to withdraw or modify his or her request. I must temporarily suspend providing an accounting of disclosures at the request of a health oversight agency or law enforcement official for a time specified by such agency or official. The agency or official should provide a written statement that such an accounting would be "reasonably likely to impede" activities and the amount of time needed for suspension. However, the agency or official statement may be made orally, in which case I will document the statement, temporarily suspend the accounting, and limit the temporary suspension to no longer than 30 days, unless a written statement is submitted.

Patient Rights - 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.

Patient Rights - 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.

Breach Notification: If an unintended breach of confidentiality occurs, I will take the following steps:
1. If I become aware of or suspect a breach, I will conduct a Risk Assessment and keep a written record of that Risk Assessment.
2. Unless I determine that there is a low probability that your information has been compromised, I will notify you of the breach of information.
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 PHI in its control, I will provide any required notice to patients and Health and Human Services.
4. 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.

Business Associates: I 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.

If I will be unavailable for an extended time, my business associate, Dr. Nicole Massey-Hastings provides clinical coverage for my practice. You will be provided with her contact information when I am away. In order to provide clinical coverage, she may have access to clinical information in order to provide appropriate emergency care. Timothy Palac, Christopher Peters, and Paula Hastings assist with technology services and business administration and may have limited access to PHI for the purposes of: technology services, business administration assistance, billing, and practice management.

Administrative Requirement—Privacy Officer: The privacy officer receives complaints and fulfills obligations as set out in notice to patients.
Privacy Officer: Catharine Devlin, Psy.D. 773-428-0959.

Administrative Requirement—Safeguards: To protect the privacy of the PHI of my patients, I have in place appropriate administrative, technical, and physical safeguards, in accordance with the Privacy Rule. I maintain an encrypted electronic record system with your personal information, diagnosis, treatment progress, and other clinical information.

Administrative Requirement—Complaints: The privacy of my patients' PHI is critically important for my relationship with my patients and for my practice. I provide a process for my patients to make complaints concerning my adherence to the requirements of the Privacy Rule.

1. Patients may file privacy complaints by submitting them in one of the following ways:
   a. In person, orally or in writing.
   b. By mail, in a letter containing the necessary information. All complaints should be mailed to:
      1300 W. Belmont Ave., Suite 508
      Chicago, IL 60657
   c. By telephone at **773-428-0959**
2. All privacy complaints should be directed to the **Catharine Devlin, Psy.D**.
3. The complaint must include the following information:
   a. The type of infraction the complaint involves
   b. A detailed description of the privacy issue
   c. The date the incident or problem occurred, if applicable
   d. The mailing/email address where formal response to the complaint may be sent.

Administrative Requirement—Mitigation: I mitigate, to the extent possible, any harmful effect that I become knowledgeable of regarding my use or disclosure, or my business associate's use or disclosure, of PHI in violation of policies and procedures or the requirements of the Privacy Rule.

Administrative Requirement—Retaliatory Action and Waiver of Rights: I believe that patients should have the right to exercise their rights under the Privacy Rule. I do not take retaliatory action against a patient for exercising his or her rights or for bringing a complaint. Of course, I will take legal action to protect myself, if I believe that a patient undertakes an activity in bad faith. I will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against a patient for exercising a right, filing a complaint or participating in any other allowable process under the Privacy Rule. I will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against a patient or other person for filing an HHS compliance complaint, testifying, assisting, or participating in a compliance review, proceeding, or hearing, under the Administrative Simplification provisions of HIPAA. I will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against a patient or other person for opposing any act or practice made unlawful under the Privacy Rule, provided that the patient or other person has a "good faith belief" that the practice is unlawful and the manner of opposition is reasonable and does not involve disclosure of PHI. I will not require a patient to waive his or her rights provided by the Privacy Rule or his or her right to file an HHS compliance complaint as a condition of receiving treatment.

Administrative Requirement—Policies and Procedures: To ensure that I am in compliance with the Privacy Rule, I have implemented policies and procedures to ensure compliance with the privacy rule. My policies and procedures are a demonstration of my compliance with the Privacy Rule. I promptly change my policies and procedures that accord with changes to the Privacy Rule and provide prompt notice to patients.

Administrative Requirement—Documentation: I meet applicable state laws and the Privacy Rule's requirements regarding documentation. I maintain policies and procedures in written or electronic form. All written communication required by the Privacy Rule is maintained (or an electronic copy is maintained) as documentation. If an action, activity, or designation is required by the Privacy Rule to be documented, a written or electronic copy is maintained as documentation. Documentation is maintained for a period of six years from the date of creation or the date when it last was in effect, whichever is later.