PATIENT RECORDS PRIVACY
POLICIES AND PROCEDURES GUIDANCE

Use and Disclosure of PHI

Policy

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 domestic violence or abuse, as required by law
- Court orders
- Workers' compensation laws
- Serious threats to health or safety
- Government oversight (including disclosures to a public health authority, coroner or medical examiner, military or veterans' affairs agencies, an agency for national security purposes, law enforcement)
- Health research
- Marketing or fundraising. However, individuals have the right to opt out of marketing and fundraising communications.
- 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

Policy

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.

- I may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose, if the PHI is requested by another covered entity, by a public official (who represents that the information requested is the minimum necessary), or by a researcher (with appropriate documentation).

- I may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose, if the PHI is requested by a member of my staff or business associate.

- 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

While a patient may authorize the release of any of his PHI, the Privacy Rule specifically requires patient authorization for the release of Psychotherapy Notes. Psychotherapy Notes authorization is different from patient consent or authorization of other PHI, because a health plan or other covered entity may not condition treatment, payment, enrollment, or eligibility for benefits on obtaining such authorization.

As defined by the Privacy Rule, "Psychotherapy Notes" means "notes recorded (in any medium) by a mental health professional, documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the individual's medical record." The term "excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date."

Policy

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
- For use or disclosure in supervised training programs where trainees learn to practice counseling
- 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 of permissible disclosure 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.

Patient Rights—Notice

Policy

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.

Procedure for Provision of Uses and Disclosures That May be Made Regarding PHI and My Duties and Patient Rights with Respect to Notice

Clients are informed that I, Melinda Goodman, PsyD, am the privacy officer in my practice.

- I provide notice to my patient on the first date of treatment. In an emergency situation, I provide notice "as soon as reasonably practicable." (This first date of treatment timing requirement applies to electronic service delivery, and a patient may request a paper copy of notice when services are electronically delivered.)

- Except in emergency situations, I make a good faith effort to obtain from a patient written acknowledgement of receipt of the notice. If the patient refuses or is unable to acknowledge receipt of notice, I document why acknowledgement was not obtained.

- 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.

- I make notice available in my office for patients to take with them and post the notice in a clear and prominent location.

- I make notice available on my website for patients to access.

Policy

As required under the Privacy Rule, and in accordance with state law, I provide notice to patients following a breach of unsecured PHI under the following conditions:

(a) there is a breach (a use or disclosure of your PHI in violation of the HIPAA Privacy Rule) involving your PHI;
(b) the 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.

<u>Procedures Related to Notification of Breach of PHI</u>

1. When the Practice becomes aware of or suspects a breach, as defined as the acquisition, access, use or disclosure of PHI in violation of the HIPAA Privacy Rule, the Practice will conduct a Risk Assessment, as outlined below and will keep a written record of that Risk Assessment.
    a. Determine the nature and extent of PHI involved.
    b. Determine to whom the PHI may have been disclosed.
    c. Determine whether the PHI was actually acquired or viewed.
    d. Determine the extent to which the risk to the PHI has been mitigated.
2. Unless the Practice determines that there is a low probability that PHI has been compromised, the Practice will give notice of the breach as described below:
    - Any patient affected by a breach will be notified without unreasonable delay and within 60 days of discovery
    - Notifications will include:
        - A brief description of the breach, including dates
        - A description of types of unsecured PHI involved
        - Steps patients should take to protect against potential harm
        - A brief description of steps taken to investigate the incident, mitigate harm, and protect against further breaches
        - My contact 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, the Practice will provide any required notice to patients and HHS.

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.

Procedure for Providing Notification of Breach to HHS

- A log of breaches occurring during the calendar year will be kept and then provided to HHS within 60 days after the year ends.

Patient Rights—Restrictions and Confidential Communications

Policy

The Privacy Rule permits patients *to request* restrictions on the use and disclosure of PHI for treatment, payment, and health care operations, or to family members. While I am not required to agree to such restrictions, I will attempt to accommodate a reasonable request. Once I have agreed to a restriction, I may not violate the restriction; however, 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.

The Privacy Rule also permits patients *to request* receiving communications from me through alternative means or at alternative locations. As required by the Privacy Rule, I will accommodate all reasonable requests.

- 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.

- 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.

- Termination of a restriction can be accepted orally or in written form; I document such termination.

Patient Rights—Access to and Amendment of Records

Policy

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

Policy

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. I also do not have to provide an accounting for disclosures made for national security purposes, to correctional institutions or law enforcement officers, or that occurred prior to April 14, 2003.

- 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.

    - A written accounting record will be provided. For each disclosure in the accounting, the following information is noted: 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. In lieu of the statement of purpose, a copy of a written request for disclosure for any of the permitted disclosures in the Privacy Rule or by HHS for compliance purposes may be provided.

    - If multiple disclosures have been made for a single purpose for various permitted disclosures under the Privacy Rule or to HHS for compliance purposes, the accounting also includes the frequency, periodicity, or number of disclosures made and the date of the last disclosure.

    - 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.

Business Associates

Policy

I may 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.

The contract also provides that the business associate will—

- Comply with the Security Rule, Privacy Rule and other provisions of HIPPA made applicable to business associates under the Final Rule.
- Ensure that any PHI that the business associate obtains, stores or processes is secured so that it does not qualify as Unsecured PHI
- Use appropriate safeguards to prevent inappropriate use and disclosure, other than provided for in the contract,
- Report as soon as practicable and in no less than 5 business days any beach or use or disclosure not provided for by its contract of which the business associate becomes aware,
- Ensure that subcontractors agree to the same contract's conditions and restrictions that apply to the business associate,
- Make records available to patients for inspection and amendment and incorporate amendments as required under the patient access and amendment of records requirements of the rule,
- Make information available for an accounting of disclosures,
- Make its internal practices, books, and records relating to the use and disclosure of PHI available to HHS for compliance reviews, and
- At contract termination, if feasible, return or destroy all PHI.

- If I know of a pattern of activity or practice of a business associate that constitutes a material breach or violation of the agreement, I will take reasonable steps to cure the breach. If such steps are unsuccessful, I will terminate the contract, or if termination is not feasible, I will report the problem to HHS.

Administrative Requirement—Privacy Officer

Policy

I am my practice's privacy officer, and am responsible for the development and implementation of the policies and procedures to protect PHI, in accordance with the requirements of the Privacy Rule. As the contact person for my practice, the privacy officer receives complaints and fulfills obligations as set out in notice to patients.

Privacy Officer Job Description

The Privacy Officer is responsible for all ongoing activities related to the development, implementation, maintenance of, and adherence to the practice's policies and procedures covering the privacy of and access to patient's PHI in compliance with federal and state laws.

Reporting Relationship: As applicable
Qualifications: Current knowledge of applicable federal and state privacy laws.
The *duties* of the Privacy Officer are as follows:

1. Develops, implements and maintains the practice's policies and procedures for protecting individually identifiable health information.
2. Conducts ongoing compliance monitoring activities.
3. Works to develop and maintain appropriate consent forms, authorization forms, notice of privacy practices, business associate contracts and other documents required under the HIPAA Privacy Rule.
4. Ensures compliance with the practice's privacy policies and procedures and applies sanctions for failure to comply with privacy policies for all members of the practice's workforce and business associates.
5. Establishes and administers a process for receiving, documenting, tracking, investigating and taking action on all complaints concerning the practices privacy policies and procedures.
6. Performs all aspects of privacy training for the practice and other appropriate parties. Conducts activities to foster information privacy awareness with the practice and related entities.
7. Ensures alignment between security and privacy practices.
8. Cooperates with the Office of Civil Rights and other legal entities in any compliance reviews or investigations.

Administrative Requirement—Training

Policy

As required by the Privacy Rule, I train all members of my staff, as necessary and appropriate to carry out their functions, on the policies and procedures to protect PHI. I have the discretion to determine the nature and method of training necessary to ensure that staff appropriately protects the privacy of my patients' records.

Administrative Requirement—Safeguards

Policy

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. All PHI are kept locked in my office. My computer has a firewall installed to protect PHI from being inspected by anyone outside of my practice.

Administrative Requirement—Complaints

Policy

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.

Procedure for a Complaint Process

1. Patients may file privacy complaints by submitting them in one of the following ways:
   a. In person, in a letter containing the necessary information.
   b. By mail in a letter containing the necessary information.

Is There a Problem

2. All privacy complaints should be directed to me.

3. The complaint must include the following information:
   a. The type of infraction involved
   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.

4. When a privacy complaint is filed by a patient the following process should be followed:
   a. Validate the complaint with the individual.
   b. If appropriate, attempt to correct any apparent misunderstanding of the policies and procedures on the patient's part; if after clarification, the patient does not

want to pursue the complaint any further, indicate that "no further action is required." Record the date and time and file under dismissed complaints.

c. If not dismissed, log the complaint by placing a copy of the letter in both the complaint file and in the patient's record.
d. Investigate the complaint by reviewing the circumstances with relevant staff (if applicable).
e. If it is determined that the complaint is invalid, send a letter stating the reasons the complaint was found invalid. File a copy of the letter and form in an investigated complaints file.
f. If the investigative findings are unclear, get a second opinion either from your lawyer, the APA Insurance Trust, or the APA Practice Organization.
g. If it is determined that the complaint is valid and linked to a required process or an individual's rights, follow the office sanction policy to the extent that an individual is responsible. If the complaint involves compliance with the standards that do not involve a single individual, then begin the process to revise current policies and procedures.
h. Once an appropriate sanction or action has been taken with respect to a complaint with merit, or if the response will take more than 30 days, send a letter explaining the findings and the associated response or intended response. Document the disposition of the complaint and file the letter and form in an investigated complaints file.
i. Place a copy of the letter in the patient's record.
j. Review both invalid and investigated complaint files periodically, to determine if there are any emerging patterns.

Administrative Requirement—Mitigation

Policy

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

Policy

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

Policy

To ensure that I am in compliance with the Privacy Rule, I have implemented policies and procedures to ensure compliance with the privacy rule.

- I promptly change my policies and procedures that accord with changes to the Privacy Rule. Notice provided to my patients must also be promptly changed to reflect the change in policy and procedure, unless the change does not materially affect the notice. The timing of the change in notice and reliance on the change may depend on the terms for such changes in the notice.

Administrative Requirement--Documentation

Policy

I meet applicable state laws and the Privacy Rule's requirements regarding documentation.

- I maintain policies and procedures in written 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.