Jonathan J. Whitfield, MD
HIPAA Privacy Rule: Policies and Procedures[1]

Under the HIPAA Privacy Rule, codified at 45 CFR § 160.101 *et seq.* ("Privacy Rule")[2], covered entities, including health care providers such as psychiatrists, must establish policies and procedures with respect to protected health information ("PHI") that set forth and implement the standards and requirements of the Privacy Rule. The policies and procedures must be reasonably designed to ensure compliance with the Privacy Rule and any amendments thereto, taking into account the size and type of activities that relate to PHI that are undertaken by the covered entity. A covered entity must:

- maintain these policies and procedures in written or electronic form;
- if, under the Privacy Rule and as set forth in the policies and procedures, a communication is required to be in writing, maintain such written communication or an electronic copy as documentation for six years; and
- if, under the Privacy Rule and as set forth in the policies and procedures, an action, activity or designation is required to be documented, maintain a written or electronic record of such action, activity or designation for six years.

The following is a detailed outline of the policies and procedures that must be maintained by an individual practitioner or small practice covered entity under the Privacy Rule.

- **Notice of Privacy Practices for PHI** – 45 CFR § 164.520 – The policies should provide, and incorporate procedures to implement, that:

  - the covered entity will make available to each patient or prospective patient a "Notice of Privacy Practices" that provides adequate notice of the uses and disclosures that may be made of individuals' PHI by the covered entity, individuals' rights with respect to the PHI, and the covered entity's legal duties with respect to the PHI, and that contains the required elements that are set forth in 45 CFR § 164.520 and incorporated in the *APA's Sample Notice of Privacy Practices (section V. A)*

  - the Notice will be provided:
    - upon request
    - in the case of patients with whom the covered entity has a direct treatment relationship, (1) no later than the date of the first service delivery, including service delivered electronically, or as soon as reasonably practicable in an emergency treatment situation, in which case the covered entity will make a good faith effort to obtain written acknowledgment of receipt of the Notice or to document the effort to obtain such acknowledgment; (2) have the Notice available at the practice site and post the Notice in a clear and prominent location easily visible to patients

---

[1] Disclaimer: This information is provided to assist APA members in complying with the federal HIPAA privacy regulation. Members should use this information to draft policies and procedures that fit their particular practices. This information is provided solely for general informational purposes and does not constitute, and should not be relied upon as, legal advice. Members should consult with attorneys to evaluate their specific circumstances and obtain customized advice, particularly with respect to drafting policies and procedures that comply with applicable state law which may, in certain cases, preempt the federal law requirements. While all reasonable attempts have been made to ensure the accuracy, completeness, and timeliness of this information, the APA disclaims any express or implied representations or warranties as to the accuracy, completeness or timeliness of this information for any purpose or suitability of this information for any particular use. Members using this information assume full responsibility for their use of it and agree that the APA is not liable for any claim, loss or damage arising from any member's use or reliance upon this information.

[2] The Privacy Rule may be accessed at http://www.hhs.gov/ocr/hipaa/finalreg.html.

and prospective patients; and (3) whenever the Notice is revised, make the Notice available upon request on or after the effective date of the revision;
- (in the case of covered entities who maintain web sites concerning their services) on or through the covered entity's web site; and
- via email if the individual agrees, provided that if email transmission fails, a paper copy of the Notice will be provided;

- the covered entity will document compliance with the Notice requirements by retaining copies of the notices issued by the covered entity, and, if applicable (as in an emergency treatment situation), retaining any written acknowledgment of receipt or documentation of good faith efforts to obtain such written acknowledgements; and

- the covered entity will not use or disclose PHI in a manner inconsistent with the Notice.

- **Designation of Privacy Official** – 45 CFR § 164.530(a)(1) – The policies and procedures should state that the covered entity will designate a privacy official who is responsible for the development and implementation of the policies and procedures of the covered entity and document who has been designated as the privacy official.

- **Uses and Disclosures of PHI - Authorizations** – 45 CFR § 164.508

  - Uses and Disclosures for which Authorization is Required – The policies and procedures should provide, and incorporate procedures to implement, that, with some exceptions, the covered entity will obtain an authorization from an individual before using or disclosing his or her PHI, and the covered entity will then only use or disclose the PHI in accordance with the authorization.

    - Psychotherapy notes – The policies and procedures should set forth the specific authorization requirements applicable to psychotherapy notes and provide an explanation of what constitutes psychotherapy notes as defined in 45 CFR § 164.501. The policies should provide that the covered entity will obtain an authorization for the use and disclosure of psychotherapy notes, except for the following uses and disclosures:
      - Use by the originator of the psychotherapy notes for treatment;
      - Use or disclosure by the covered entity in its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family or individual counseling;
      - Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual;
      - Use or disclosure to the Secretary of the Department of Health and Human Services as required to investigate or determine compliance with the Privacy Rule;
      - Use or disclosure as required by law;
      - Use or disclosure as permitted under the Privacy Rule for the oversight of the originator of the psychotherapy notes;
      - Use or disclosure as permitted by the Privacy Rule to a coroner or medical examiner;
      - Use or disclosure as permitted by the Privacy Rule to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

    - Marketing – If applicable, the policies and procedures should set forth the specific authorization requirements applicable to uses or disclosures of PHI for marketing purposes and provide an explanation of what constitutes marketing as defined in 45 CFR § 164.501. The policies should provide that a covered entity will obtain an authorization for any use or disclosure of PHI for marketing, except if the communication is in the form of: (1) a face-to-face communication made by the covered entity to an individual; or (2) a promotional gift of nominal value provided by the covered entity. The policies should further provide that if the marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization from the individual for use of his or

her PHI must state that such remuneration is involved.

- Fundraising – If applicable, the policies and procedures should set forth that:
  - the covered entity will obtain an authorization for the use or disclosure of PHI for fundraising, except if the disclosure is to a business associate or to an institutionally related foundation and is only of demographic information of an individual and the dates of health care provided to an individual for the purpose of raising funds for the covered entity; and
  - the covered entity will include in any fundraising materials it sends to an individual a description of how the individual may opt out of receiving future fundraising communications, and the covered entity will make reasonable efforts to ensure that those individuals who choose to so opt out are not sent future fundraising communications.[3]

- Exceptions to Authorization Requirement – The policies should set forth the following situations, in which the covered entity is not required to obtain an individual's authorization to use or disclose such individual's PHI, and the guidelines for implementation in connection with each:
  - When carrying out treatment, payment or health care operations (except in the case of psychotherapy notes or PHI used in marketing) [See 45 CFR § 506];
  - To the individual who is the subject of the PHI;
  - For facility directories (but requires giving the individual an opportunity to agree or object to use and disclosure) [See 45 CFR § 164.510(a)];
  - To family members or other persons involved in the individual's care (but requires giving the individual an opportunity to agree or object to use and disclosure) [See 45 CFR § 164.510(b)];
  - For disaster relief purposes (but requires giving the individual an opportunity to agree or object to use and disclosure) [See 45 CFR § 164.510(b)(4)];
  - As required by law [See 45 CFR § 164.512(a)];
  - For public health activities [See 45 CFR § 164.512(b)];
  - About victims of abuse, neglect or domestic violence [See 45 CFR § 164.512(c)];
  - For health oversight activities [See 45 CFR § 164.512(d)];
  - For judicial and administrative proceedings [See 45 CFR § 164.512(e)];
  - For law enforcement purposes [See 45 CFR § 164.512(f)];
  - About decedents [See 45 CFR § 164.512(g)];
  - For cadaveric organ, eye or tissue donation [See 45 CFR § 164.512(h)];
  - For research purposes [See 45 CFR 164.512(i)];
  - To avert a serious threat to health or safety [See 45 CFR § 164.512(j)];
  - For specialized governmental functions [See 45 CFR § 164.512(k)];
  - For workers' compensation [See 45 CFR § 164.512(l)]; and
  - To the Secretary of the Department of Health and Human Services when required to enforce the Privacy Rule.

- Other Policy Provisions re-Authorizations – The policies should set forth, and incorporate procedures to implement, the following:
  - a description of the elements required to make an individual's authorization valid as provided in 45 CFR § 164.508(c) and incorporated (*see the APA's Sample Authorization to Use and Disclose Health Care Information located in section V. C);*

---

[3] APA encourages psychiatrists to offer patients the opportunity to opt out of receiving fundraising communications, prior to receiving such communications. This can practicably be done as part of the Notice of Privacy Practices, and documented in the patient's record.

- a description of the defects in an authorization that will make such authorization invalid, *i.e.*, expiration date or event has passed, incomplete authorization, revoked authorization, violates a requirement of the Privacy Rule regarding conditioning of authorizations or compound authorization, or contains false material information of which the covered entity is aware;
- that an authorization for use and disclosure of PHI may not be combined with any other document to create a compound authorization, except:
    - an authorization for use and disclosures of PHI for research may be combined with other types of written permission for the same study;
    - an authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes; and
    - an authorization, other than an authorization for psychotherapy notes, may be combined with any other authorization except when a covered entity has conditioned the provision of treatment on the provision of one of the authorizations;
- that the covered entity can not condition the provision of treatment on the provision of authorization, except in the case of research-related treatment or the provision of health care solely for the purpose of creating PHI for disclosure to a third party, such as in the case of pre-employment mental health assessments;
- that an individual may revoke an authorization at any time by revoking it in writing, except when the covered entity has taken action in reliance upon the authorization;
- that if the covered entity seeks an authorization from the individual, the covered entity will provide the individual with a copy of the signed authorization; and
- that the covered entity will document and retain any signed authorizations.

- **Other Requirements Relating to Uses and Disclosures of PHI**

    - **Minimum Necessary** – 45 CFR § 164.502(b), 164.514(d) – The policies should state, and incorporate procedures to implement, the following:
        - when using or disclosing PHI, or when requesting PHI from another covered entity, the covered entity will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request;
        - the minimum necessary requirement does not apply to the following:
            - disclosures to or requests by a health care provider for treatment;
            - uses and disclosures made to the individual as permitted or required under the Privacy Rule, as in an accounting of disclosures or when the individual has requested access to his or her PHI;
            - uses or disclosures made pursuant to an authorization by an individual;
            - disclosures made to the Secretary of the Department of Health and Human Services;
            - uses or disclosures that are required by law; and
            - uses or disclosures required to comply with the Privacy Rule;
        - the covered entity will take steps to ensure the implementation of the minimum necessary standard as follows:
            - identify persons in the covered entity's workforce who need access to PHI to carry out their duties, identify the categories of PHI to which access is needed, and make reasonable efforts to limit such persons' access to only such PHI;
            - limit any request for PHI made by the covered entity to that which is reasonably necessary to accomplish the purpose for which the request is made when requesting such information from other covered entities;
            - for routine and recurring disclosures of PHI or requests for disclosure of PHI by the covered entity, establish procedures that limit the PHI disclosed or requested to the amount reasonably necessary to achieve the purpose of the disclosure;

- for other types of disclosures or requests for disclosures of PHI, develop criteria designed to limit the PHI disclosed or requested to the information reasonably necessary to accomplish the purpose for which the disclosure is sought or for which the request is made, and review requests for disclosure on an individual basis in accordance with such criteria;
- not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request;

- the covered entity may rely on a request for disclosure as being for the minimum necessary amount of information if:
  - the disclosure is to a public official permitted under the Privacy Rule, and such official represents that the request is for the minimum necessary information;
  - the request is from another covered entity;
  - the request is from a professional in the covered entity's own workforce or from a business associate in order to provide a professional service for the covered entity, and the requestor represents that the request is for the minimum necessary information; or
  - the requestor provides documentation or representations that meet the requirements for use and disclosure of the PHI for research purposes as set forth in 45 CFR § 164.512(i).

- **Verification of Identity and Authority** – 45 CFR § 164.514(h) – The policies should provide, and set forth procedures to implement, that:
  - prior to making any disclosure of PHI, the covered entity will verify the identity and the authority of the requesting party to have access to such PHI, including obtaining any necessary documentation as required by the Privacy Rule to make such verification, unless:
    - the identity or authority of the person to receive the PHI is known to the covered entity;
    - the disclosure is for a facility directory, to family members or other persons involved in the individual's care, or for disaster notification purposes, in which case the individual must be given an opportunity to object or agree to such disclosures (see 45 CFR § 164.510) and the verification requirement will be met if the covered entity exercises professional judgment in making such a disclosure; or
    - the disclosure is to avert a serious threat to health or safety (see 45 CFR § 164.512(j) and in which case the verification requirement will be met if the covered entity acts on a good faith belief in making such disclosure; and
  - the covered entity will verify the identity and authority of a public official requesting disclosure of PHI in accordance with 45 CFR § 164.514(h)(2)(ii).

- **Personal Representatives** – 45 CFR § 164.502(g) – The policies should set forth, and incorporate procedures to implement, that the covered entity will:
  - treat a personal representative of an individual as if he or she is the individual;
  - treat a person who has the authority to act on behalf of an adult or an emancipated minor in making health care decisions as the personal representative of such person with respect to PHI;
  - treat a person who has the legal authority to act on behalf of an unemancipated minor in making health care decisions (*e.g.*, a parent or guardian) as the personal representative of such minor with respect to PHI relevant to such personal representation, unless:
    - the minor is permitted by law to consent to the health care service, and the minor has so consented and not requested that the person be treated as the personal representative;
    - the minor may lawfully obtain such health care service without the consent of a parent or guardian, and the minor has consented to the service; or

- a parent or guardian assents to an agreement of confidentiality between the health care provider and the minor with respect to such health care service.

The policies and procedures should further provide, however, that despite these exceptions with respect to unemancipated minors, the covered entity:

- may disclose PHI to a parent or guardian if applicable state law or other law permits such disclosure;
- may not disclose PHI to a parent or guardian if applicable state law or other law prohibits such disclosure; and
- may provide or deny access to PHI to a parent or guardian who is not the personal representative in accordance with the covered entity's professional judgment if state law or other law does not address the issue.

- treat an executor, administrator or other person who has the authority to act on behalf of a deceased individual or of the individual's estate as the personal representative of the individual with respect to PHI relevant to such personal representation;
- may elect, if warranted, not to treat a person as the personal representative of an individual if the covered entity has a reasonable belief that:
  - the individual has been or may be subjected to domestic violence, abuse or neglect by such person; or
  - treating such person as the personal representative could endanger the individual; and
  - in the exercise of professional judgment, the covered entity decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

- **Deceased Persons** – 45 CFR § 164.502(f) – The policies and procedures should provide that the covered entity will comply with the requirements of the Privacy Rule with respect to the PHI of deceased persons and set forth procedures to implement such compliance.

- **De-Identification of PHI** – 45 CFR §§ 164.520(d), 164.514(a) – Generally, there is no requirement for a covered entity to make available de-identified PHI, to which the requirements of the Privacy Rule for individually identifiable health information are not applicable. Therefore, a covered entity could choose to implement a policy stating that it does not de-identify data. However, if a covered entity decides to de-identify information, it must follow the requirements in the Privacy Rule and establish policies and procedures in accordance with the Privacy Rule as set forth in 45 CFR § 164.514(a).

- **Limited Data Sets** – 45 CFR § 164.514(e) – There is no requirement that a covered entity make available a limited data set, as defined under the Privacy Rule, for the purposes of research, public health, or health care operations, which would involve the disclosure of information concerning an individual that excludes a significant amount of confidential data. Therefore, a covered entity could choose to implement a policy stating that it does not provide limited data sets. However, it is permissible under the Privacy Rule to provide limited data sets if the covered entity so chooses, in which case the covered entity must follow the requirements of the Privacy Rule and develop a policy setting forth the requirements of the Rule as set forth in 45 CFR § 164.514(e).

- **Access by Individuals to PHI** – 45 CFR § 164.524 – The policies and procedures should provide, and incorporate procedures to implement, that:
  - with some exceptions, an individual has the right to inspect and obtain a copy of his or her PHI maintained by the covered entity;
  - the covered entity will permit such requests for access to PHI and may require such requests in writing;

- with respect to requested PHI that is maintained by the covered entity or is accessible to the covered entity on-site, the covered entity will, within 30 days of receiving such request, take one of the following steps:
  - grant the request in whole or in part, inform the individual, and provide the access requested;
  - deny the request in whole or in part in writing;
  - if the covered entity is unable to act on the request within the 30 day period, provide the individual with a written statement extending the time in which it will act on the request by no more than 30 days, setting forth the date by which it will complete its action on the request, and giving the reasons for the delay;
- with respect to requested PHI that is not maintained or accessible by the covered entity on-site, within 60 days of receiving such request, take one of the three steps described in the above bullet point regarding on-site requested PHI;
- if the covered entity grants the requested access, it:
  - will provide the individual with the right to inspect or obtain a copy of the PHI or both;
  - will provide the PHI in the form or format requested by the individual if it is readily producible in such form or format, or, if not so readily producible, in such form as agreed upon by the individual and the covered entity;
  - will arrange with the individual a convenient time and place to inspect or obtain a copy of the PHI or mail a copy of the PHI at the individual's request;
  - may charge a reasonable, cost-based fee for the cost of copying the PHI and any applicable postage;
  - may provide a summary of the PHI in lieu of the actual PHI, as long as the individual has agreed in advance to such summary and to any reasonable, cost-based fee the covered entity may charge for preparing such summary;
  - may provide an explanation of the PHI to which access has been provided, as long as the individual has agreed in advance to such explanation and to any reasonable, cost-based fee the covered entity may charge for preparing such explanation;
- the covered entity may deny individuals access to PHI <u>without</u> providing the individual an opportunity for review of such denial in the following circumstances:
  - the request is for psychotherapy notes;
  - the request is for information compiled in reasonable anticipation of or for use in a civil, criminal or administrative proceeding;
  - the request is for information maintained by the covered entity that is subject to or exempted from the Clinical Laboratory Improvements Amendments of 1988 (CLIA);
  - the request is for information maintained by the covered entity acting under the direction of a correctional institution and providing a copy of the PHI to the individual would jeopardize the health, safety, security, custody or rehabilitation of the individual, other inmates, officers, or other persons at the institution;
  - while research is in progress, when the request is for information obtained by a provider in the course of research that includes treatment of the research participants;
  - the request is for information also subject to the Privacy Act and denial is permitted under the Privacy Act; or
  - if the covered entity obtained the requested PHI from someone other than a health care provider under a promise of confidentiality and such access would be reasonably likely to reveal the source of the information;
- the covered entity may deny individuals access to PHI <u>with</u> the opportunity for review of such denial in the following circumstances:
  - if access is reasonably likely to endanger the life or physical safety of the individual or another person;
  - the request is for PHI that references another person and disclosure is reasonably likely to cause substantial harm to such other person; or
  - the request is made by the personal representative of the individual and disclosure is reasonably likely to cause substantial harm to the individual or another person;
- in the case of denials with a right to review, the individual will have the right to have such denial reviewed by a licensed health care professional who is designated by the covered entity and who

did not participate in the original denial decision; the covered entity will provide written notice to the individual of the determination of the reviewing professional and will comply with the reviewing professional's determination;

- if the covered entity denies, in whole or in part, the requested access, it:
  - will make available any PHI to which access has not been denied;
  - provide a timely written, plain language denial explaining the basis for the denial, the individual's rights to review of the denial, if applicable, how the individual may exercise such rights, and how the individual may complain to the covered entity, including the name or title and telephone number of the contact person or office, or to the Secretary of the Department of Health and Human Services;
- if the covered entity does not maintain the PHI that is the subject of the individual's request for access and the covered entity knows where such PHI is maintained, the covered entity will inform the individual where to direct his or her request; and
- the covered entity will document and retain the records that are subject to access by individuals and the title of the persons or offices responsible for receiving and processing requests for access by individuals.

- **Amendment of PHI** – 45 CFR § 164.526 – The policies and procedures should provide, and incorporate procedures to implement, that:
  - an individual has the right to have the covered entity amend his or her PHI for as long as the PHI is maintained by the covered entity, except if the PHI that is subject of the request (1) was not created by the covered entity (unless the individual shows that the originator of the PHI is no longer available to act on the requested amendment, in which case the covered entity should address the requested amendment as if the covered entity had created the PHI); (2) is not part of the covered entity's record; (3) would not be available for the individual's inspection under the Privacy Rule; or (4) is accurate and complete;
  - the covered entity will permit an individual to request the covered entity to amend the PHI it maintains and may, with advance notice to individuals, require a written request for amendment and statement of the reason for the requested amendment;
  - the covered entity will respond to an individual's request for amendment within 60 days of receipt of the request by doing one of the following:
    - granting the request for amendment and taking the steps described below to incorporate the amendment;
    - denying the requested amendment in whole or in part; or
    - if the covered entity is unable to act on the request within the 60 day period, providing the individual with a written statement extending the time in which it will act on the request by no more than 30 days, setting forth the date by which it will complete its action on the request, and giving the reasons for the delay;
  - the covered entity will, in the case of accepting the requested amendment, take the following steps:
    - amend the PHI or, at a minimum, identify the affected PHI and append the amendment;
    - inform the individual of the granting of the requested amendment and obtain the individual's permission to notify others with a need to know of the amendment;
    - make reasonable efforts within a reasonable time to inform and provide the amendment to (1) persons identified by the individual as possessing PHI and needing the amendment; and (2) persons that the covered entity knows have the PHI that is the subject of the amendment and that have relied or could rely on such PHI to the detriment of the individual;
  - the covered entity will, in the case of denying the requested amendment, provide the individual with a written denial explaining:
    - the basis for the denial,
    - the individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
    - that if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the requested amendment; and

        - how the individual may complain to the covered entity, including the name or title and telephone number of the contact person or office, or to the Secretary of the Department of Health and Human Services;
    - the covered entity will permit an individual to submit to the covered entity a written statement disagreeing with the denial of all or part of the request for amendment, and, if the covered entity chooses, reasonably limiting the length of such statement;
    - the covered entity may choose to prepare a written rebuttal to an individual's statement of disagreement with a denial of a requested amendment, in which case it will provide a copy of such rebuttal to the individual;
    - the covered entity will identify the PHI in the individual's record that is the subject of the disputed amendment and append the individual's request for amendment, the covered entity's denial, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any;
    - the covered entity will include in future disclosures of the PHI to which a disagreement concerning amendment relates:
        - if the individual has submitted a statement of disagreement, either (1) the individual's request for amendment, the covered entity's denial, the individual's statement of disagreement, and the covered entity's rebuttal, if any; or (2) an accurate summary of such information; or
        - if the individual has not submitted a statement of disagreement and only if the individual has requested that such information be included in future disclosures of the PHI, either (1) the individual's request for amendment and the covered entity's denial; or (2) an accurate summary of such information;
    - the covered entity will amend an individual's PHI in its records when it is informed by another covered entity of an amendment to such PHI in accordance with the Privacy Rule; and
    - the covered entity will document and retain the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals.

- **Accounting of Disclosures** – 45 CFR § 164.528 – The policies should provide and incorporate procedures to implement that:
    - an individual has the right to receive an accounting of all disclosures of his or her PHI, except when the disclosures are:
        - To carry out treatment, payment or health care operations;
        - To individuals of PHI about them;
        - Incident to a disclosure or use permitted or required under the Privacy Rule;
        - Pursuant to a valid authorization;
        - For notification purposes, such as for the covered entity's facility directory, if any, or to persons involved in the individual's care;
        - For national security or intelligence purposes;
        - To correctional institutions or law enforcement;
        - As part of a limited data set in accordance with Section 164.514(e) of the Privacy Rule;
        - Made prior to the Privacy Rule compliance date; or
        - Made more than six years prior to the request for accounting of disclosures;
    - the covered entity will temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official where such accounting would impede the agency's activities as detailed in 45 CFR § 164.528(a)(2);
    - the covered entity will maintain accountings of disclosures of PHI as set forth in 45 CFR § 164.528(b) and provided in the *APA's Sample Form for Accounting of Disclosures of Protected Health Information located in section V. E*);
    - the covered entity will disclose the accountings of disclosures when requested by the individual and determined to be appropriate;
    - the covered entity will act upon the individual's request for an accounting no later than 60 days after receipt of such a request by either providing the individual with the accounting requested or, if the covered entity is not able to provide the accounting within such 60 days, a written statement extending the time in which the accounting will be provided by no more than 30 days, setting forth the date by which the accounting will be provided, and giving the reasons for the delay;

- the covered entity will provide the first accounting to an individual in any 12 month period without charge, and may, with advance notice to the individual, establish a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period; and
- the covered entity will document and retain the documentation of (1) the information required to be included in an accounting; (2) the written accounting that is provided to an individual; and (3) the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

- **Business Associates** – 45 CFR § 164.504(e) – The policies should state, and incorporate procedures to implement, that prior to disclosing PHI to any business associate or permitting a business associate to create or receive PHI on its behalf, the covered entity will require the business associate to enter into a written contract or other agreement that requires the business associate to appropriately safeguard the PHI as required by the Privacy Rule and contains the required elements as are set forth in 45 CFR § 164.504(e) and incorporated in the *APA's Sample Business Associate Contract in section V. D*). The policy should further provide that a business associate contract will not be required in the case of disclosures by the covered entity to another health care provider concerning the individual.

- **Right of Individual to Request Restriction of Certain Uses and Disclosures of PHI by Covered Entity** – 45 CFR § 164.522(a) – The policies should state, and incorporate procedures to implement, that:
  - an individual has the right to request that the covered entity restrict its uses or disclosures of the individual's PHI when carrying out treatment, payment or health care operations and when communicating with persons involved in the individual's care, but that the covered entity is not required to agree to any such requested restrictions;
  - if the covered entity chooses to agree to such a restriction, the covered entity will document such restriction and not use or disclose PHI in violation of such restriction, except (1) in the case of an emergency, in which case the covered entity will request that the recipient health care provider not redisclose the PHI; or (2) in the case of disclosures of de-identified information, disclosures for facility directories or disclosures of PHI permitted without authorization under 45 CFR § 164.512 of the Privacy Rule; and
  - a covered entity may terminate its agreement to a restriction if:
    - the individual agrees or requests the termination in writing;
    - the individual orally agrees to the termination and such agreement is documented; or
    - the covered entity informs the individual in advance that it is terminating its agreement to a restriction.

- **Right of Individual to Request Confidential Communications** – 45 CFR § 164.522(b) – The policies should state, and incorporate procedures to implement, that:
  - an individual may request and the covered entity will accommodate reasonable requests by individuals to receive communications of PHI from the covered entity by alternative means or at alternative locations;
  - the covered entity may require the individual to make the request for confidential communications:
    - in writing;
    - with the provision of information as to how payment, if any, will be handled; and
    - with a specification of an alternative address or other method of contact for the individual; and
  - the covered entity will not require the individual to provide an explanation of the basis for his or her request for confidential communications as a condition of providing communications confidentially.

- **Complaint Procedure** – 45 CFR § 164.530(d) – The policies and procedures should detail the process the covered entity has established for individuals to make complaints concerning the covered entity's policies and procedures or its compliance with such policies and procedures, including the contact

person or office the covered entity has designated to receive complaints and provide further information about matters covered in the Notice of Privacy Practices. Such procedures should include a process for documenting all complaints received and their disposition, if any.

- **Safeguards for PHI** – 45 CFR § 164.530(c) – The policies and procedures should state that the covered entity will implement administrative, technical, and physical safeguards to reasonably protect the privacy of PHI, including safeguarding it from intentional or unintentional disclosures in violation of the Privacy Rule, and limiting incidental uses or disclosures of PHI made pursuant to a permitted use or disclosure, and describe such safeguards.[4]

- **Training** – 45 CFR § 164.530(b) – The policies should state, and incorporate procedures to implement, that:
  - the covered entity will provide training to all members of its workforce about the policies and procedures concerning PHI as necessary and appropriate for the members of the workforce to carry out their functions within the practice;
  - such training will be provided to existing members of the covered entity's workforce no later than the compliance date for the practice, to each new member within a reasonable period of time after the person joins the workforce, and to each member of the practice's workforce whose functions are affected by a material change in the policies or procedures within a reasonable time after the change becomes effective; and
  - the covered entity will document that the required training has been provided.

- **Mitigation** – 45 CFR § 164.530(f) – The policies and procedures of a covered entity should provide that the covered entity will mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies or procedures or the Privacy Rule by the covered entity or any of its business associates.

- **Sanctions** – 45 CFR § 164.530(e) – The policies and procedures should state:
  - the sanctions that the covered entity has implemented and will use with respect to members of its workforce who fail to comply with the policies and procedures or the Privacy Rule; and
  - that the covered entity will document sanctions that are imposed, if any.

- **Refraining from Intimidating or Retaliatory Acts** – 45 CFR § 164.530(g) – The policies and procedures should provide that the covered entity will refrain from intimidating, threatening, coercing, discriminating against, or taking other retaliatory action against any individual for exercising his or her rights under the Privacy Rule or opposing any act or practice in violation of the Privacy Rule, provided that such opposition is based on good faith belief of a violation, is exercised reasonably, and does not involve disclosure of PHI in violation of the Privacy Rule.

- **No Requiring Waiver of Rights** – 45 CFR § 164.530(h) – The policies and procedures should provide that a covered entity will not require individuals to waive their rights under the Privacy Rule as a condition of treatment.

Patients' Acknowledgment of Receipt of Notice of Privacy Practices*[5]

---

[4] Note: Specific safeguard requirements for PHI are not included in the Privacy Rule, but will be specified in a separate security rule that has not yet been finalized, but which will, once finalized, allow reasonable time for compliance. A proposed security rule, entitled Security and Electronic Signature Standards, 63 Fed. Reg. 43242, was published in August 1998.

[5] **Disclaimer**: This information is provided to assist APA members in complying with the federal HIPAA privacy regulation. Members should use this information to draft policies and procedures that fit their particular practices. This information is provided solely for general informational purposes and does not constitute, and should not be relied upon as, legal advice. Members should consult with attorneys to evaluate their specific circumstances and obtain customized advice, particularly with respect to drafting policies and procedures that comply with applicable state law which may, in certain cases, preempt the

Jonathan J. Whitfield, MD

Patient Name: _____ **Birth date**:_____
Maiden /other name (if applicable):_____

I acknowledge that I have received a copy of the Notice of Privacy Practices of **Jonathan J. Whitfrield, MD,** effective _____.

Signature (patient or authorized representative):_____

Date: _____

Relationship/authority (if signed by authorized representative):
_____