KERN AUGUSTINE CONROY & SCHOPPMANN, P.C.
Attorneys to Health Professionals
info@DrLaw.com • DrLaw.com • 800-445-0954

HIPAA PRIVACY POLICY & PROCEDURE MANUAL

DISCLAIMER

This document was prepared to assist the typical physician practice in seeking to undertake reasonable measures to comply with the HIPAA Rules. Each practice must review this document for individualized adaptation to your practice or to a particular transaction. While it has been drafted to provide accurate and authoritative assistance in the development of your HIPAA compliance program, it is not intended as, and does not constitute, legal or other professional advice, which can be rendered only on an individual practice and fact-sensitive basis. This guidance is based on the law and regulations in force at the time of publication. Users should consult experienced health care counsel for individualized and ongoing guidance regarding the specific and evolving application of the HIPAA rules to their practice, as well as for evolving state privacy and security law compliance requirements. Under the HITECH Act, the majority of the new HIPAA statutory provisions became effective February 18, 2010. However, the Office for Civil Rights, which enforces HIPAA, did not issue a final rule until January 25, 2013. The final rule provides covered entities and business associates with 180 days beyond the effective date (March 26, 2013) of the final rule to come into compliance with its mandates. This means that, with the exception of some business associate agreements, Covered Entities must have policies and procedures and compliant forms and agreements in place, and staff training completed, as of September 23, 2013.

Romanelli Cosmetic Surgery
North Shore Plastic Surgery
******

HIPAA PRIVACY POLICY & PROCEDURE MANUAL

Dated: 9/6/2013

HIPAA PRIVACY POLICY & PROCEDURE MANUAL

Table of Contents

HIPAA PRIVACY POLICY & PROCEDURE MANUAL

INTRODUCTION

A. *What is the HIPAA Privacy Rule?*

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") was enacted by Congress. HIPAA included what are called "Administrative Simplification" provisions that required the U.S. Department of Health and Human Services ("HHS") to adopt national standards for electronic health care transactions, such as health care claims that are filed electronically. Because advances in electronic technology could make it difficult to protect the privacy of health information, Congress mandated the adoption of the HIPAA Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule" or "Rule"). Congress subsequently enacted the HIPAA Security Rule and, more recently, the Health Information Technology for Economic and Clinical Health (HITECH) Act. In addition, the state has enacted laws regarding identity theft prevention, data security breach notification and protected use and disclosure of Social Security numbers (see our Practice's Data Breach Notification Policy). The Rule does not replace other federal, state or other laws that give individuals even greater privacy protections, and are no pre-empted by the Privacy Rule.

The Privacy Rule establishes national protections for the privacy of protected health information ("PHI"), and applies to three types of HIPAA covered entities: health plans, health care clearinghouses, and health care providers, like our Practice, that conduct certain health care transactions electronically. The Rule requires that Covered Entities implement policies and procedures to protect and guard against the misuse of PHI. This Policy Manual reflects our commitment to compliance with the Privacy Rule.

B. *Our Privacy Officer*

The Privacy Rule requires that we designate a person who will serve as our "Privacy Officer" and who is responsible for the development and implementation of our privacy policies and procedures. We must also designate a person to serve as the contact person responsible for receiving complaints under the Privacy Rule and who can make further information available to patients about matters covered by our Notice of Privacy Practices.

We have designated our **MANAGING PHYSICIAN** as the Privacy Officer for our Practice, to be responsible for the development and implementation of our privacy policies and procedures, and to be the contact person to answer questions and receive complaints related to our privacy practices.

C. *Definitions*

Our Policy Manual has a Glossary that explains many terms used in the Manual. Every staff person should review and consult the Glossary when reviewing or consulting this Policy Manual.

Capitalized words in the Policy Manual are defined in the Glossary.

D. *What does HIPAA Privacy mean to our Practice and our Workforce?*

Each member of our Workforce needs to understand what our basic Privacy Policies and Procedures are and how to request help if further information is needed. We will make a copy of our Policy Manual available to each member of our Workforce and require that each member review the policies and our Notice of Privacy Practices and participate in training we offer on the Privacy Rule. If the Privacy Rule changes, or new guidance is issued that requires a change in our Policy Manual, we will have each member of our Workforce review the changed policies. Together we will commit to providing quality health care to our patients, while maintaining the privacy of their protected health information and complying with the Privacy Rule.

NOTICE OF PRIVACY PRACTICES

Policy Number 1
HIPAA §164.520, 164.514

Policy: The HIPAA Privacy Rule provides that patients have a right to notice of how we may use and disclose a patient's PHI, as well as the patient's rights and our obligations regarding their PHI. We have developed a Notice of Privacy Practices to meet these requirements and will make the Notice available to our patients as described in this policy. Our Practice will strive to abide by the terms of our Notice as currently in effect.

Procedure:

1. Content of Notice

Our Notice of Privacy Practices ("Notice") has been written in plain language to contain all of the elements required by the Privacy Rule, including the following:

A. A description of how we use and disclose patients' PHI, including:

i. A description, with at least one example, of the types of uses and disclosures that we are permitted to make for treatment, payment, and health care operations;

ii. A description of each of the other purposes for which we are permitted or required by HIPAA to use or disclose PHI without the patient's written authorization;

iii. A statement that other uses and disclosures will be made only with the patient's written authorization (see Policy No. 3 of this Policy Manual); and

iv. If applicable to our operations, a statement that we may use or disclose certain PHI for fundraising communications but that the patient will have the opportunity to opt out of future fundraising communications as specified in the communication made to the patient.

B. A description of the individual rights of our patients regarding access and control of their PHI, and how a patient may exercise those rights, including:

i. The right to request restrictions on certain uses and disclosures and whether our Practice is required to agree to a requested restriction, including agreeing to the request of a patient to restrict disclosure of PHI about him/her to a health plan if the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise

required by law and the PHI pertains solely to a health care item or service for which the patient, or person other than the health plan, has paid us in full for the item or service;

ii. The right to receive certain confidential communications;

iii. The right to inspect and obtain a copy of PHI;

iv. The right to request an amendment of PHI;

v. The right to receive an accounting of certain disclosures of PHI;

vi. The right to revoke an authorization;

vii. A description of our complaint procedure for addressing problems the patient may have with our privacy practices;

viii. The right to obtain a paper copy of the Notice, upon request;

ix. If we maintain an electronic health record, the right to: a) access to or obtain a copy of PHI in an electronic form and format requested by the patient, if it is readily producible or, if not, in a readable electronic form and format as agreed to between us and the patient; b) have us transmit such copy directly to a person or entity the patient designates, provided that choice is clear, conspicuous, and specific; c) request that we provide an accounting of the disclosures we have made of the patient's PHI (including disclosures related to treatment, payment and health care operations) contained in an electronic health record for no more than 3 years prior to the date of the request (and depending on when we acquired an electronic health record); and

x. Notice of any allowed fees related to the above.

C. A description of our legal duties regarding PHI, including our legal obligation to maintain the privacy of PHI and our obligation to notify affected individuals following a breach of their unsecured PHI.

D. Identification of whom in our Practice a patient may contact for more information about our privacy practices.

E. The effective date of the Notice and any revisions of the Notice, with the effective date of such revisions.

2. <u>Providing the Notice</u>

A. We will present the Notice to each patient at their first date of service delivery by

us and will make a good faith attempt to obtain each patient's acknowledgment of receipt of the Notice.

i. We will have a patient acknowledge receipt by signing an acknowledgment form.

ii. If the patient refuses to provide such acknowledgment, we will document in the patient's chart our efforts to obtain the patient's acknowledgment and the reason why the acknowledgment was not obtained.

iii. If there is an emergency treatment situation, we will provide the Notice to the patient as soon as reasonably practicable after the emergency situation. No acknowledgment of receipt of the Notice need be obtained in an emergency situation.

B. We will post our entire current Notice in a prominent location in our office(s).

C. We will provide a paper copy of the Notice upon a patient's request.

D. When our first treatment encounter with a patient is not face-to face, we will follow the following procedures:

i. If we first treat a patient over the telephone (not simply obtain information to schedule an appointment or procedure), we will mail the Notice to the patient the same day, if possible, with a request to sign an enclosed acknowledgment and return it to our office. We will maintain a file copy of the acknowledgment form sent to the patient as documentation of our efforts to obtain the patient's acknowledgment, in case the patient fails to return the acknowledgment form.

ii. We may e-mail our Notice to a patient if the patient agrees to receive an electronic notice. An electronic return receipt will serve as the patient's acknowledgment of receipt of the Notice.

iii. If our first service delivery to a patient is provided over the Internet, through e-mail, or otherwise electronically, we will send an electronic notice automatically and contemporaneously in response to the patient's first request for service. An electronic return receipt will serve as the patient's acknowledgment of receipt of the Notice.

E. If the patient has a personal representative acting on the patient's behalf at the time Notice is provided, we will provide the Notice to the representative and make a good faith effort to obtain the representative's acknowledgment of receipt of the Notice.

3. Revisions to our Notice

A. Our Practice will advise patients in the Notice that we reserve the right to change the terms of the Notice and to make the new Notice provisions effective for all PHI that we maintain.

B. We will review our Notice at least annually. If we determine at any time that there is a material change to our privacy practices, or there is a change in law that requires a change in our Notice, we will revise our Notice, date it with the effective date of the revision, post the revised Notice in our office(s), then implement the changes (unless a change in law requires that we implement the change sooner), and provide the revised Notice pursuant to this Policy. We will advise patients in our Notice that they can obtain a revised Notice upon request on or after the effective date of any revision. No acknowledgement is necessary for providing a revised Notice to a patient who has received a prior version of our Notice. Patients can access our revised Notice on our website, if we maintain one.

4. We may utilize a "layered" Notice that consists of a short notice summarizing the patient's rights, attached to a longer notice that contains all of the elements listed in Subsection 1 of this Policy. The patient will be provided with the two documents stapled together, with the shorter notice on top of the longer notice.

5. If we participate in an Organized Health Care Arrangement and utilize a single, joint notice with another health care provider, our Privacy Officer will determine the requirements related to such joint notice.

6. Documentation

A. Our Privacy Officer will maintain a file containing a copy of our Notice and every revised Notice that is issued by our Practice.

B. We will place in the patient's medical record a copy of the acknowledgment of receipt (which will also contain a reference to the version of the Notice they received), whether provided by hard copy or electronically, or documentation of our good faith efforts to obtain such written acknowledgment.

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION NOT REQUIRING PATIENT AUTHORIZATION

Policy Number 2
HIPAA §§164.502, 506, 512, 514

Policy: Our Practice may use and disclose PHI in certain situations where it is not necessary to obtain the patient's authorization, as allowed under the Privacy Rule. We will follow Policy No.4 of this Policy Manual (regarding application of the Minimum Necessary principle) whenever using or disclosing PHI without patient authorization.

Procedure: In the following situations, our Practice may use or disclose PHI without obtaining the patient's authorization:

1. For Treatment, Payment or Health Care Operations:

A. A patient's authorization is not required when we use or disclose the patient's PHI for our purposes in order to treat the patient, obtain payment for our services, or conduct our own business operations, including disclosure to our business associates (as further described in this Manual).

i. We will, nevertheless, in order to ensure compliance with state law and any payor mandates, obtain a patient's authorization naming the patient's health insurer (including any employee, agent or subcontractor of the insurer) as an authorized representative of the patient for purposes of receiving the patient's PHI as necessary for us to obtain payment for our services (applying our Policy No. 4 regarding our Minimum Necessary principle).

ii. A patient is permitted to request, in writing, that we restrict the uses or disclosures of his or her PHI for treatment, payment or health care operations, or when disclosing information to persons involved in the patient's care, or for notification purposes. Except as set forth below, we are not required to agree to the patient's request, but we are bound by any restrictions to which we agree unless and until we withdraw from such agreement, where permitted. Such requests shall be directed to our Privacy Officer.

If a patient requests that we restrict the disclosure of the patient's PHI to their health plan, our Practice must comply if:

a. The disclosure is not for purposes of carrying out treatment (only for purposes of carrying out payment or health care operations); and
b. The PHI pertains solely to a health care item or service for which

our Practice has been paid out-of-pocket in full.

iii. A patient is permitted to request, in writing, that the patient receive communications of PHI from us by alternative means or at alternative locations (other than the usual way we send communications to our patients). We must accommodate a patient's reasonable request for such confidential communications. Such requests shall be directed to our Privacy Officer.

iv. Special rules apply if the patient's file contains psychotherapy notes, if we intend to use the PHI for marketing purposes or if we intend to use PHI in a manner that would be considered a Sale of PHI (see Glossary of Terms). Such cases shall be referred to our Privacy Officer.

B. We may disclose PHI for the treatment activities of another health care provider. Where PHI is disclosed to, or requested by, other health care providers for Treatment purposes, our minimum necessary policy (Policy No. 4) does not apply.

C. We may disclose PHI to another Covered Entity for the peer review activities of that entity, subject to review and approval by our Privacy Officer.

D. If we are part of an Organized Health Care Arrangement ("OHCA,"), we may disclose PHI to other participants in the OHCA for any health care operations activities of the OHCA. Such disclosures, or requests for such disclosures, shall be referred to our Privacy Officer.

E. Any use or disclosure of PHI for Treatment, Payment or Health Care Operations must be consistent with our current Notice of Privacy Practices.

F. Consistent with our Notice of Privacy Practices, we may use certain PHI, or disclose certain PHI to a business associate or to an institutionally related foundation, for the purpose of raising funds for our own benefit. Any such communication to the patient will tell the patient in a clear and conspicuous manner how he or she may opt out of receiving future fundraising communications from us, without undue burden or more than nominal cost, as well as how to opt back in to receive such communications. We will not condition treatment or payment on the patient's choice regarding receipt of fundraising communications and we will not make fundraising communications to a patient who has elected not to receive them.

2. Required Uses and Disclosures Not Requiring Patient Authorization

Other than for disclosures to the patient, no disclosure under this Section 2 shall be made without the prior review and approval of our Privacy Officer who may consult with our legal counsel.

A. To the Patient. Under the law, except as provided in Policy No. 6 of this Policy Manual, we must make disclosures *to the patient* who requests such disclosure and no authorization is required. If the patient requests a copy of his or her record, refer to Policy No. 6 of this Policy Manual.

B. To the Secretary of HHS. We must make disclosures of PHI when required by the Secretary of HHS or to OCR to investigate or determine our compliance with the requirements of the Privacy Rule.

C. As Required By Law. To the extent that the use or disclosure of PHI is required by an applicable law, we may do so without the patient's authorization, in compliance with, and limited to, the relevant requirements of such law.

D. Public Health Activities. We may use or disclose a patient's PHI, without the patient's authorization, for the following public health activities and purposes:

i. Public Health Authorities: Disclosure to a public health authority that is legally authorized to receive such information for the purpose of preventing or controlling disease, injury or disability, such as reporting of injury or communicable disease; vital events such as birth and death; public health surveillance; public health investigation; and public health intervention; or, if directed by the public health authority, to a foreign government agency that is collaborating with the public health authority.

ii. Communicable Diseases. In addition to reporting communicable disease information to a public health authority as provided for in Subsection D.i, above, we may disclose a patient's PHI, as authorized by state law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease or condition.

iii. Abuse or Neglect.

a. Children: We may disclose a patient's PHI to a public health authority that is authorized by law to receive reports of child abuse or neglect.

b. Adults: Except for vulnerable adults, if we believe that an adult patient has been a victim of abuse, neglect or domestic violence, we may disclose a patient's PHI to the governmental entity or agency authorized by law to receive such information. No disclosure of information about the victim of domestic violence or abuse may be made to law enforcement without the patient's authorization.

c. Vulnerable Adults: When we believe a vulnerable adult is the

subject of abuse, neglect or exploitation, we may disclose the patient's PHI to the appropriate government adult protective services provider.

iv. Food and Drug Administration. We may disclose a patient's PHI to a person or entity authorized by the U.S. Food and Drug Administration ("FDA") to receive information related to the quality, safety or effectiveness of an FDA-regulated product or activity for which the person or entity has responsibility.

v. Workplace Medical Surveillance. We may disclose PHI to an individual's employer without the individual's authorization only in very specific circumstances where the individual is a member of the employer's workforce and we provide health care to the individual at the request of their employer to conduct an evaluation related to medical surveillance of the workplace or an evaluation to determine whether the individual has a work-related illness or injury. (Note that, where the employer is requesting an evaluation of an individual for purposes other than those stated in this Subsection, or otherwise allowed in this policy, or where some third party other than the individual's employer is requesting an evaluation of the individual, we will follow our Policy No. 3 regarding uses and disclosures requiring an authorization.)

E. Health Oversight. We may disclose PHI to a health oversight agency for activities authorized by law, such as audits; civil, criminal or administrative investigations, proceedings or actions; inspections; or licensure or disciplinary actions.

F. Legal Proceedings. We may disclose PHI in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (but only that PHI for which disclosure is expressly authorized), and, under certain conditions, in response to a subpoena, discovery request or other lawful process. Workforce members should direct all subpoenas, and other requests for disclosures for purposes of legal proceedings, to our Privacy Officer who may consult our legal counsel.

G. Law Enforcement. We may disclose PHI for law enforcement purposes, without a patient's authorization, so long as specific legal requirements are met. Some of these law enforcement purposes include: warrants and other legal process; limited information requests for identification and location purposes; and information related to a crime (including a medical emergency where it is likely that a crime has occurred).

H. Coroners, Medical Examiners, Funeral Directors, and Organ Donation.

i. We may disclose PHI to a coroner or medical examiner for identification

purposes, determining cause of death or for the coroner or medical examiner to perform other official duties.

ii. We may disclose PHI to a funeral director, as authorized by state law, in order to permit the funeral director to carry out his or her duties, including disclosure prior to, and in reasonable anticipation of, the death of a patient, if necessary for the funeral director to carry out his or her duties.

iii. We may use a patient's PHI, or disclose a patient's PHI to appropriate entities engaged in the procurement, banking or transplantation of cadaveric organs, eyes or tissue, for the purpose of facilitating such activities, as authorized under state law.

I. Research. If our Practice is called upon to use or disclose PHI for research purposes, such use and disclosure will be under the direction of our Privacy Officer who shall consult with our Practice's legal counsel.

J. Serious Threat to Health or Safety. Under certain circumstances, we may use a patient's PHI, or disclose it to another health care professional or to a law enforcement agency, if we believe, in good faith, that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or to others or is necessary in certain situations for law enforcement authorities to identify or apprehend an individual who is a serious threat to public safety. If the PHI contains identifying information about a person who has AIDS or an HIV infection, we will not disclose such information without the patient's authorization, unless authorized by state law, or pursuant to a court order.

K. Specialized Government Functions. When the appropriate conditions apply, we may use or disclose a patient's PHI for certain military, national security or intelligence activities, or when needed for correctional institutions and other law enforcement custodial situations.

L. Workers' Compensation. A patient's PHI may be disclosed by us as authorized under state law to comply with workers' compensation laws and other similar programs established by law that provide benefits for work-related injuries or illness without regard to fault. If we routinely make disclosures for workers' compensation purposes, we have developed standard protocols for those disclosures as part of our minimum necessary policy and procedures (see Policy No. 4).

M. Schools; Immunization Records. We may disclose a patient's PHI to a school when the patient is a student or a prospective student of the school if: (i) the PHI that is disclosed is limited to proof of immunization, (ii) the school is required by state law (or other law) to have proof of immunization prior to admitting the individual and (iii) we obtain and document the oral agreement for such disclosure from the parent, guardian or other person acting *in loco parentis* of an

unemancipated minor or from the individual, if the individual is an adult or emancipated minor.

3. Verification of the Identity of an Authorized Person

A. Prior to any disclosure of PHI under this policy, we will verify the identity of the person requesting the PHI and the authority of any such person to have access to the patient's PHI, if the identity or any such authority of the person is not known to us.

B. We will obtain and/or document any pertinent credentials, documentation, statements or representations, whether oral or written, from the person requesting the PHI.

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION REQUIRING PATIENT AUTHORIZATION

Policy Number 3
HIPAA §§164.508, 514

Policy: Our Practice may use or disclose a patient's PHI for those purposes specified in Policy No. 2 without obtaining the patient's authorization. Other uses and disclosures of PHI, as addressed in this policy, will be made only with the patient's written authorization. Our Practice will not condition treatment on the provision by the patient of a requested authorization except as allowed under this policy.

Procedure:

1. Whenever our Practice needs to use or disclose a patient's PHI for purposes unrelated to Treatment, our Payment or Health Care Operations (or as otherwise described in Policy No. 2), or if a patient requests disclosure of his or her PHI to a specified third party, we will obtain the patient's prior written authorization for such use or disclosure.

2. We will only release that PHI consistent with the scope of the authorization.

3. Authorization Form: Our Practice's authorization form shall provide for the following:

    A. The name of the person or entity, or category of persons/entities authorized to make the requested use or disclosure;

    B. The name of the person or entity, or category of persons/entities, to whom the use or disclosure may be made;

    C. Specifically describe the information to be used or disclosed, including, but not limited to, specific detail such as date of service, type of service provided, level of detail to be released, origin of information, etc.;

    D. List the specific purposes for the use or disclosure. If the individual does not, or elects not to, provide a statement of the purpose, the form will state the purpose as "at the request of the individual";

    E. Specify that the authorization will be in force and effect until a specified date or event (stated in the authorization) that relates to the patient or to the purpose of the use or disclosure, at which time the authorization will expire;

    F. Provide for the patient's right to revoke the authorization as set forth in Subsection 4, below;

G. Specify that our Practice will not condition treatment upon the patient's execution of an authorization, as set forth in Subsection 5, below;

H. Specify that the information disclosed pursuant to the authorization may be re-disclosed by the recipient and no longer subject to the protections of the Privacy Rule; and

I. Provide for the patient's signature and date of execution or, if the patient's Personal Representative is signing on behalf of the patient, provide for a description of that person's authority to act and/or that person's relationship to the patient.

4. Revocation of Authorization

A. A patient has the right to revoke an authorization at any time, in writing, by mailing such written notification to the attention of our Practice's Privacy Officer or by personal delivery to our Privacy Officer.

B. A revocation is not effective to the extent that our Practice has taken action in reliance on the patient's authorization.

5. Our Practice will not condition a patient's treatment on whether the patient provides authorization for the requested use or disclosure if to do so would be prohibited by federal or state law. If a reason exists under law for conditioning the patient's treatment on obtaining an authorization, the patient will be advised of that fact and of the consequences to the patient of refusing to sign the authorization. Our Privacy Officer will determine if such reason exists.

6. Independent Medical Examination. In accordance with state law, if a third party has requested that our Practice examine or evaluate a person ("Examinee") and the Examinee has signed an authorization for the release of our report of such examination or evaluation to the third party:

A. The report shall be consistent with the authorization, to avoid unnecessary disclosure of diagnoses or personal information which is not pertinent to the evaluation;

B. The report shall be forwarded only to the third party who requested the evaluation, in accordance with the Examinee's authorization and, if no specific individual is identified, the report shall be marked "Confidential"; and

C. We shall not provide the Examinee with a copy of the report unless the third party requesting the examination consents to its release, except that should the examination disclose abnormalities or conditions not known to the Examinee, we will advise the Examinee to consult another health care professional for treatment.

7. If an authorization is being requested for PHI that contains psychotherapy notes, we will refer the matter to our Privacy Officer for complying with such request in accordance with law.

8. If an authorization is being requested for PHI for marketing purposes, we will refer the matter to our Privacy Officer for complying with such request in accordance with law.

9. If an authorization is being requested for PHI for research purposes, we will refer the matter to our Privacy Officer for complying with such request in accordance with law.

10. If an authorization is being requested for a use or disclosure considered a sale of PHI, we will refer the matter to our privacy officer for complying with such request in accordance with law.

11. We shall not directly or indirectly receive remuneration in exchange for any PHI of a patient unless we have obtained from the patient a valid authorization that includes a specification of whether the PHI can be further exchanged for remuneration by the entity receiving the patient's PHI. This requirement shall not apply if the purpose of the exchange is:

    a. For public health activities;
    b. For research and the price charged reflects the costs of preparation and transmittal of the data for such purposes;
    c. For treatment and payment purposes;
    d. For the sale, transfer, merger or consolidation of all or part of our Practice with another Covered Entity, and due diligence related to such activity;
    e. For remuneration that is provided by our Practice to a Business Associate for activities involving the exchange of PHI that the Business Associate undertakes on our behalf and at our specific request pursuant to a Business Associate Agreement;
    f. To provide a patient with a copy of the patient's PHI pursuant to Policy 6 of this Manual;
    g. As required by law; or
    h. For any other purpose permitted by or in accordance with the Privacy Rule where the only remuneration received by our Practice is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

    Any offer of remuneration in exchange for PHI shall be directed to our Privacy Officer.

12. Prior to any disclosure of PHI under this policy, we will verify the identity of the person requesting the PHI and the authority of any such person to have access to the patient's PHI, if the identity or any such authority of the person is not known to us. We will obtain any documentation, statements or representations, oral or written, from the person requesting the PHI when such documentation, statement or representation is pertinent to the disclosure.

13. We can accept a government agency's authorization form as long as it meets the requirements of Subsection 3, above.

14. The patient may receive a copy of the authorization, upon request.

15. Our Practice will document in the patient's medical record that the patient's authorization was obtained for the specific use or disclosure and shall retain the signed authorization in the patient's medical chart, in either written or electronic form, for at least six years from the date when it last was in effect. If the patient revokes the authorization, we will document such revocation in the patient's medical record and retain the signed revocation in the same manner as an authorization.

"MINIMUM NECESSARY" IN PHI USE, DISCLOSURE, AND REQUEST

Policy Number 4
HIPAA ' '164.502(b), 514(d)

Policy: Except as otherwise stated in this policy, whenever we use or disclose PHI, or when we request PHI from another Covered Entity or Business Associate, our Practice will make reasonable efforts to limit the information, to the extent practicable, to the Limited Data Set or, if needed by our Practice, to the Aminimum necessary@ to accomplish the intended purpose of the use, disclosure or request, respectively. At such time as the Secretary of HHS issues guidance on what constitutes "minimum necessary," we will follow that guidance when applying this Policy.

Procedure:

1. Exceptions to this policy

Our uses and disclosures of PHI, and requests for PHI, that are *not* subject to this policy requiring that the minimum necessary information be used or disclosed, are as follows:

A. Disclosures to or requests by a health care provider for Treatment purposes, including our own requests for disclosure of PHI for Treatment purposes;

B. Disclosures made to the patient, including but not limited to disclosures made to the patient pursuant to the patient=s request to access his or her record or for an accounting of disclosures made by our Practice of the patient=s PHI;

C. Uses or disclosures made pursuant to a patient's authorization that meets the requirements of our Policy No. 3;

D. Disclosures made to the Secretary of HHS related to enforcement of the requirements of the HIPAA privacy standard;

E. Uses or disclosures required by other law as described in Policy No. 2 of this Policy Manual;

F. Uses or disclosures that are required for compliance with the requirements of the HIPAA privacy standard; or

G. PHI that has been De-identified, as specified in the Privacy Rule.

2. Situations Where this Policy Does Apply

A. Our Own Use of PHI

i. Our Practice has established which persons or categories of persons in our Practice need access to PHI to carry out their duties.

ii. For each such person or category, we have determined the types of PHI to which access is needed, including identification of those persons or classes of persons in our Practice who need to see the entire medical record, and any conditions that exist for access (role-based access).

iii. We will make reasonable efforts to limit the access only to the amount of information needed by the person in order to carry out the duties of that position or to accomplish the required use.

B. Our Own Disclosures of PHI

For disclosures of PHI that we make on a *routine and recurring* basis, we have established a standard protocol for limiting the PHI disclosed to the minimum amount reasonably necessary to achieve the purpose of the disclosure.

For *non-routine* disclosures, we have developed criteria designed to limit the PHI disclosed to the minimum information reasonably necessary to accomplish the purpose of the disclosure. We will review requests for such *non-routine* disclosures on an individual, case-by-case basis for conformance with these criteria.

The criteria for *non-routine* disclosures do not need to be applied when a request for disclosure is received in the following situations and the request appears to reasonably limit the disclosure to the minimum necessary under the particular circumstances of the request:

i. Requests for disclosures received from a health care provider, health plan or health care clearinghouse;

ii. Requests for disclosures received from public officials in those situations identified in Policy No. 2 (No Authorization Required) of this Policy Manual and the public official represents that the information requested is the minimum necessary;

iii.. Requests for disclosures received from a professional member of our Practice, or from one of our business

associates for the purpose of providing professional services to our Practice, if the professional represents that the information requested is the minimum necessary for the stated purpose; or

iv. Requests for disclosures received from a researcher with appropriate documentation from an Institutional Review Board or Privacy Board.

C. For both routine and non-routine disclosures and requests, we have identified in our protocol the circumstances under which the entire medical record is reasonably necessary for particular purposes.

D. We will reasonably rely on requests from the business associate of another health care provider, health plan or health care clearinghouse for the disclosure of PHI as meeting the minimum necessary requirement for the intended purpose.

3. Our Own Requests for PHI

We will limit any request for PHI that we make to another health care provider, a health plan, or a health care clearinghouse to that which is reasonably necessary to accomplish our purposes.

For requests made on a *routine and recurring* basis, we have established a protocol that limits the PHI requested to the amount reasonably necessary to accomplish our purposes.

For requests on a *non-routine or non-recurring* basis, we have developed criteria designed to limit the request for PHI to the information reasonably necessary to accomplish our purposes. We will review such non-routine requests on an individual basis for conformance with these criteria.

Our Practice will make reasonable expenditures to implement technologically feasible approaches in complying with this Aminimum necessary@ policy. (See Policy No. 9 (Safeguarding PHI).

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION WHERE THE PATIENT HAS AN OPPORTUNITY TO AGREE OR OBJECT

Policy Number 5
HIPAA §§164.510, 514

Policy: Our Practice may use and disclose PHI in certain situations where it is necessary or beneficial to involve others in the patient's health care or to notify others of the patient's status or condition. In these situations, the patient has the opportunity to agree or object to the use or disclosure of all or part of the patient's PHI for these purposes.

Procedure:

1. We may make the following disclosures for involvement in the patient's care and notification purposes:

    A. Disclosing to a Family Member, other relative, close personal friend of the patient, or any other person identified by the patient, PHI that is directly relevant to that person's involvement in the patient's health care or payment related to the patient's health care; or

    B. Using or disclosing PHI to notify, or assist in the notification of, a Family Member, a Personal Representative of the patient or another person who is responsible for the patient's care, of the patient's location, general condition or death.

    C. Disclosing PHI to any person identified in 1A, above, who was involved in the patient's care or payment for the patient's health care prior to the patient's death, PHI of the patient that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to us.

2. If the patient is present or otherwise available prior to our using or disclosing their PHI in this way, and the patient has the capacity to make health care decisions, we will only disclose the information if we:

    A. Provide the patient with the opportunity to agree or object to the disclosure, and the individual does not express an objection (we can inform the patient orally and accept the patient's oral agreement or objection, but we will document such agreement or objection in the patient's medical record); or

    B. Can reasonably infer from the circumstances, based on the exercise of

professional judgment, that the patient does not object to the disclosure.

3. If the patient is not present, or it is impractical to offer the patient the opportunity to agree or object to a use or disclosure of their PHI in these situations, because the individual is incapacitated or an emergency exists:

   A. We may use our professional judgment to determine whether the disclosure is in the best interests of the patient; and

   B. If we determine disclosure is appropriate, will disclose only that PHI which is directly relevant to the person's involvement in the patient's care or payment related to the patient's health care or needed for notification purposes.

4. If the patient is not present, we may use our professional judgment and experience with common practice to allow another person acting on the patient's behalf to pick up medical supplies, x-rays or other similar forms of PHI because it is in the patient's best interest.

5. We may use or may disclose a patient's PHI to a public or private entity authorized to assist in disaster relief efforts for coordinating with them in notifying Family Members or other individuals involved in the patient's health care. In such situations, we will still follow the procedures of Subsections 2 through 4 of this Policy if, in our professional judgment, to do so will not interfere with the ability to respond to the emergency circumstances.

6. Patient Requests Special Restrictions on Disclosures to Others

   A patient may request that we restrict disclosures otherwise allowed under this Policy. Any such requests will be directed to our Privacy Officer.

ACCESS OF INDIVIDUALS TO PROTECTED HEALTH INFORMATION

Policy Number 6
HIPAA §164.524

Policy: Our Practice, in accordance with this policy, will provide a patient the right to inspect and obtain a copy of the patient's PHI for as long as our Practice maintains the information.

Procedure:

1. General Procedure

   A. A patient of our Practice can request to inspect and/or obtain a copy of their PHI that we maintain in a Designated Record Set and we will provide such access, unless access is to be limited as required in this Policy.

   D. A Personal Representative of a patient may also be permitted to access the patient's PHI, in accordance with this Policy.

   E. If we do not maintain the PHI that is the subject of the request, and we know where the requested information is maintained, we will inform the patient where to direct the request for access.

2. Requests for Access and Responding to Requests

   A. All requests for inspection and/or copying of a patient's PHI must be in writing. Patients will be advised of this requirement in our Notice of Privacy Practices. These requests will be directed to our Privacy Officer.

   B. We may choose to provide a summary of the requested information. Patients will be advised in our Notice of Privacy Practices of this alternative. We may only provide a summary of the PHI if the patient agrees in advance to receive a summary of their PHI and to the fee we would charge for a summary of the PHI.

   C. Our Practice will respond to a request for inspection or copying within thirty (30) days of receipt of the written request.

   D. If the patient requests, we will mail the copy of the PHI or the summary of the PHI, as agreed upon, to another person specified by the patient if the patient's request is in a writing signed by the patient and clearly identifying the designated person and where to send the copy of the PHI.

E If we maintain an electronic health record that contains the PHI requested by the patient, the patient has the right to obtain a copy of that information in an electronic form and format they request, if it is readily producible or, if not, in a readable electronic form and format as agreed between us and the patient. In addition, the patient may choose to direct us to transmit such copy directly to an entity or person designated by the patient, provided that any such choice is clear, conspicuous, and specific.

F. We will charge a fee for the copy of the patient's PHI or for a summary of the PHI) that is reasonable and cost-based, including in all cases any charge limits imposed by state law. Any fee we impose for providing a copy or summary of PHI in an electronic form shall not be greater than our labor costs in responding to the request and the supplies for creating the electronic media if the individual requests that the electronic copy be provided on portable media, again as limited by state law. Patients will be notified in our Notice of Privacy Practices that a fee will be charged and patients will be advised of the fee.

G. Our Practice will not refuse to provide a patient with a copy of his or her medical record due solely to the fact that the patient has an outstanding balance with the Practice, when it is known to us that the record is needed by another health care professional for the purpose of rendering care to the patient. In all other cases, the copying fee must be paid prior to or at the time the copy is provided to the patient or personal representative.

H. If the patient requests only to inspect his or her PHI, we will arrange with the patient for a convenient time (no later than 30 days from the request) and place (at our office or wherever the record is kept) for the inspection to take place. All inspections of PHI by patients or personal representatives shall be under the personal supervision of a designated member of our staff.

I. If any state or federal agency or official, by subpoena or by demand for statement in writing under oath or otherwise, requests a patient's PHI, our Privacy Officer will contact our legal counsel immediately.

3. <u>Denying or Limiting Access</u>

A. Our Practice may deny or limit access to a patient's PHI, *without any right to a review* of our decision, if the information:

iii. Is psychotherapy notes;

iv. Has been compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding;

v. Is that of an inmate in a correctional institution and our physician was acting under the direction of the correctional institution, and certain circumstances exist which prohibit providing a copy of PHI to the inmate (to be determined by our Privacy Officer);

vi. Was obtained by our Practice in the course of research that includes treatment of the research participant, while the research is in progress, under certain circumstances (to be determined by our Privacy Officer);

vii. Is subject to the Privacy Act, as required by that Act; or

viii. Was obtained by our Practice from someone other than a health care provider, under a promise of confidentiality, and the requested access would be reasonably likely to reveal the source of the information.

B. Our Practice may deny or limit access to a patient's PHI, *with the right to a review* of our decision, in the following situations:

i. A licensed health care professional in our Practice has determined that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

ii. The information references another person (unless such other person is a health care provider) and a licensed health care professional has determined that the access requested is reasonably likely to cause substantial harm to that other person;

iii. Access is requested by a personal representative of the patient and a licensed health care professional has determined that access by that person is reasonably likely to cause substantial harm to the patient or another person; or

iv. A licensed health care professional has reason to believe that the patient's mental or physical condition will be adversely affected upon being made aware of the subjective information contained in the PHI (or a summary of the PHI); in this case, however, the PHI can be provided, if requested by the patient (with an accompanying notice setting forth the reasons for the original refusal) directly to the patient's attorney, another licensed health care professional, the patient's health insurance carrier (through an employee of the carrier), or to a governmental reimbursement program or to an agent of such program who has responsibility to review utilization and/or quality of care.

C. The determination of whether to deny or limit access based on the grounds in Subsections 3A or 3B, above, shall be made by a licensed physician of our Practice (or, if a physician is unavailable, by another licensed health care practitioner of our Practice), in conjunction with our Privacy Officer.

D. Our Practice will provide a patient with a written notice of denial or limitation of access (see Forms section of this Manual) which shall contain: the reason for such

denial or limitation; a statement of the patient's right to a review of the denial, if such right exists; how to exercise the review rights; and a description of our complaint procedures (see Policy No. 14 of this Policy Manual), including the name or title and telephone number of our Privacy Officer as the contact person.

E. If we deny the patient access to some of his or her PHI, we will, to the extent possible, give the patient access to any other of the patient's PHI requested by the patient, where no grounds exist to deny such access.

4. Appeal of a Decision to Deny Access

A. A patient may request a review of a denial of access that was made based on one of the reasons under Subsection 3B above.

B. Requests for review of a denial of access shall be directed to our Privacy Officer who shall promptly refer the request for review by the person designated pursuant to subsection C, below.

C. Review of the denial of access shall, within a reasonable period of time, be performed by a licensed health care professional designated by our Practice and who did not participate in the original decision to deny access. Where available, another licensed physician of the Practice shall conduct such review. Where another licensed physician of the Practice is not available, another licensed health care practitioner of the Practice shall conduct the review. Where no other physician or licensed health care practitioner of the Practice exists or is available, the review will be conducted by another health care professional designated by our Privacy Officer.

D. Our Practice will conduct the review within a reasonable period of time and will attempt to conduct the review within 30 days of the request for review. Once the review is complete, we will promptly provide a written response (see Forms) to the patient setting forth the decision of the reviewing professional and shall provide access or deny access based on that decision.

E. We will maintain a copy of the inspection/copying request form in the patient's medical record, including documentation on the form of our response, and the results of any appeal and review that may have occurred.

ACCOUNTING FOR DISCLOSURES OF PROTECTED HEALTH INFORMATION

Policy Number 7
HIPAA §164.528

Policy: Our Practice will provide patients with an accounting of disclosures of their PHI as required under federal and state law and regulations.

Procedure:

1. A patient of our Practice may request and has a right to receive an accounting of disclosures our Practice has made of the patient's PHI, except as limited by this Policy. A patient may request an accounting for a time period of up to six (6) years prior to the date of his or her request. The accounting shall include disclosures made to or by our business associates. Such requests must be in writing and shall be directed to our Privacy Officer.

2. No accounting need include disclosures that we made:

   - To carry out Treatment, Payment or Health Care Operations ("TPO") of our Practice, except as set forth in subsection 3, below;
   - To patients about their own PHI;
   - Pursuant to an authorization made by the patient or the patient's personal representative regarding the patient's PHI;
   - To individuals involved in the patient's care or for other allowed notification purposes;
   - Incident to a use or disclosure otherwise permitted or required by the Privacy Rule and this Policy Manual;
   - For any facility directory maintained by our Practice;
   - For national security or intelligence purposes;
   - To correctional institutions or law enforcement officials; or
   - As part of a Limited Data Set

3. If we use or maintain an electronic health record with respect to the PHI, the accounting must include disclosures made for Treatment, Payment and Health Care Operations of our Practice but only for a time period of up to three (3) years prior to the date of the patient's request. If we had acquired an electronic health record as of January 1, 2009, we need only provide an accounting of TPO disclosures made by us from such record on and after January 1, 2014. If we acquired an electronic health record after January 1, 2009, we must provide an accounting of TPO disclosures made by us from such record on and after the later of the following: (i) January 1, 2011; or (ii) the date that we acquire an electronic health record.

4. In order to provide this accounting to our patients, our Practice will maintain a log or

record of all disclosures, other than those excluded under Section 2 above, of a patient's PHI, for a six (6) year period (or for three (3) years if an electronic health record is used or maintained), along with a copy of every accounting made to a patient.

5. A request for an accounting of disclosures shall be acted upon within sixty (60) days of receipt of the request. A one-time thirty (30) day extension may be allowed if the patient has been notified, within the initial 60-day period, of the reasons for the delay and the date by which we will provide the accounting. We may choose to provide an accounting of all disclosures made by our Practice and by any Business Associate acting on our behalf; or an accounting of all disclosures made by our Practice and provide to the patient a list of all Business Associates acting on our behalf, including contact information for such Business Associates (such as mailing address, phone, and email address), in which case such Business Associates shall provide an accounting of their disclosures upon a request made by our patient directly to the Business Associate. Our Privacy Officer shall determine which option we choose.

6. For each disclosure for which we are required to provide an accounting under this Policy, we shall maintain the following information and shall provide the information in the accounting to the patient:

A. The date of the disclosure;

B. The name of the entity or person who received the PHI and, if known, the address of such entity or person;

C. A brief description of the PHI disclosed; and

D. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request by the Secretary for a disclosure to investigate or determine our compliance with the HIPAA privacy standard or a written request received for a disclosure made under our Policy No. 2 (Disclosures Where No Authorization is Required).

7. If, during the period covered by the accounting, we have made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting may provide:

A. The information required in Section 6 of this Policy for the first disclosure during the accounting period;

B. The frequency, periodicity, or number of the disclosures made during the accounting period; and

C. The date of the last such disclosure during the accounting period.

8. If any disclosures of a patient's PHI involved a particular research purpose, our Privacy

Officer shall determine the manner of our log of disclosures and the manner of disclosing the accounting to the particular patient.

9. The first accounting provided to a patient in any 12-month period shall be without charge. We will charge a reasonable, cost-based fee for each subsequent request for an accounting by the same patient within the 12-month period, provided that we have informed the patient in advance of the fee and provided the patient with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

10. We will temporarily suspend a patient's right to receive an accounting of disclosures we have made to a health oversight agency or law enforcement official (see Policy No. 2 of this Policy Manual), for the time specified by such agency or official, if such agency or official has provided us with a written statement that such an accounting to the patient would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required. If the agency or official statement is made orally, we will:

    A. Document the statement, including the identity of the agency or official making the statement;

    B. Temporarily suspend the patient's right to an accounting of disclosures subject to the statement; and

    C. Limit the temporary suspension to no longer than thirty (30) days from the date of the oral statement, unless the appropriate written statement is submitted to us by the agency or official during that time.

AMENDMENT OF PROTECTED HEALTH INFORMATION

Policy Number 8
HIPAA §164.526

Policy: Our Practice, in accordance with this policy, will provide our patients the opportunity to request amendment of their PHI that we maintain and, where appropriate under this policy, the right to have their PHI amended.

Procedure:

1. Receiving and Acting Upon a Request for Amendment

A. A patient of our Practice can request to have his or her PHI amended. Our Notice of Privacy Practices will advise our patients that such a request must be in writing and must state a specific reason supporting the requested amendment.

B. All requests for amendment of PHI shall be directed to our Privacy Officer.

C. Action upon the request for amendment should occur within sixty (60) days of receipt. A one-time extension of not more than thirty (30) days may be allowed if our Practice, before the end of the initial sixty-day period, provides a written notice to the requestor of the reason for the delay and the date by which our Practice intends to complete its action on the request. The Privacy Officer shall track the progress of each request for amendment to attempt to ensure compliance with these timeframes.

D. Our Privacy Officer will review the amendment request for the following elements:

i. The reason for the requested amendment, such as how the information is incorrect or incomplete;

ii. Whether the requested amendment is to: 1) administrative information; and/or 2) medical information, including the source, if known, the date(s) of service, and the specific provider of service;

iii. Whether our Practice was the originator of the information; and

iv. The specific wording requested to correct the alleged inaccuracy or incompleteness.

E. Our Privacy Officer shall make a preliminary determination regarding whether an amendment request should be honored, and shall then consult with the physician,

other health care professional, or administrative staff person of our Practice who provided the care and/or made the entry that is the subject of the amendment.

i. If that physician, health care professional or administrative staff person agrees with the Privacy Officer's preliminary determination, the Privacy Officer shall obtain final approval from an Officer of the Practice.

ii. If such final approval is obtained, the Privacy Officer shall proceed with the amendment or denial of amendment, pursuant to this policy.

iii. If a determination as to whether to accept or deny the amendment cannot be made internally, the Privacy Officer shall notify the Practice's legal counsel and request a resolution of the disagreement.

2. Denying a Request for Amendment

A. Our Practice may deny a request for an amendment in the following situations:

i. Our Practice did not create the information, unless the patient provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;

ii. The information is not part of our records for a patient;

iii. The information would not otherwise be available for inspection (see Policy Number 6 regarding Access to PHI); or

iv. Our Practice determines that the information in dispute is neither inaccurate nor incomplete.

B. If our Practice determines to deny a request for amendment, in whole or in part, our Privacy Officer shall provide written notice to the requestor, within the timeframe stated in Subsection 1B this Policy, advising of the decision to deny amendment, stating the reason for the denial, and advising of our complaint procedures (see Policy No. 14 of this Policy Manual).

i. The written notice shall also advise the requestor that the individual may submit to our Privacy Officer a written statement of disagreement with the denial, stating the basis for such disagreement.

ii. In most cases, the length of the statement of disagreement will be limited to one (1) page, unless it is unreasonable in the particular circumstance to impose such a limit.

C. If the patient does not submit a statement of disagreement, the patient may request that we provide the patient's request for amendment, and the denial, with any

future disclosures of the PHI that is the subject of the requested amendment.

D. If a statement of disagreement is received from a requestor, our Privacy Officer, in consultation with the pertinent physician, health care professional or administrative staff person, shall determine whether to prepare a rebuttal statement. If a rebuttal statement is prepared, we will provide a copy to the requestor.

E. The denial--and the disagreement and rebuttal statement, if any--shall be linked to the PHI in dispute by physically attaching these documents to the disputed information in the patient's record.

F. Whenever the disputed information is disclosed to another person or entity, the information shall include the denial and, if any exists, the statement of disagreement and the rebuttal.

i. Alternatively, we can provide a summary of any of the foregoing information.

ii. If the patient has not submitted a statement of disagreement, we will include the patient's request for amendment and our denial, or a summary of the information, with any future disclosure of the patient's PHI only if the patient has requested such action.

iii. If such a subsequent disclosure is made using a standard transaction under the HIPAA Transaction Rule that cannot accommodate the denial, disagreement and rebuttal, our Practice shall separately disclose the denial, disagreement, and rebuttal to the recipient of the transaction.

3. Accepting the Request for Amendment

A. If a determination is made to make the requested amendment, our Privacy Officer shall provide written notification to the requestor that the requested amendment has been approved and the exact wording of the amendment.

B. The Privacy Officer shall seek the requestor's identification of, and agreement to, the relevant persons identified by our Privacy Officer as persons or entities with whom the amendment needs to be shared.

C. The requestor shall have ten (10) days to object to the form of amendment or to the persons with whom the amendment will be shared. If no objection is received within that time period, the amendment shall be made in the PHI and the identified parties notified.

D. Our Privacy Officer will identify the records in the designated record set for the patient that are affected by the amendment and append or otherwise provide a link

to the location of the amendment.

E. Our Privacy Officer shall, within a reasonable period of time (but no longer than thirty (30) days), take reasonable efforts (such as send written notification by certified mail, return receipt requested) to provide the exact wording of the amendment to:

i. Such persons or entities that the patient has identified as having received the relevant portion of the patient's PHI from our Practice; and

ii. Such persons, including our business associates, who we have identified as having received the relevant portion of the patient's PHI from our Practice and who may have relied, or could foreseeably rely, on such information to the detriment of the patient.

4. Making the Amendment

A. Our Privacy Officer, or his or her designee, shall identify all media forms in which the Practice maintains the information to be amended, i.e., paper, microfiche, microfilm, automated data processing or other electronic medium, and shall cross check across all systems and applications maintained by the Practice to ensure that the amendment is made, stored (as necessary), and susceptible to audit trails.

B. In no case shall the Privacy Officer, a physician or any other person of our Practice delete, erase, "white out" or otherwise obliterate medical information in a patient's record. Any correction or addition to a patient's PHI shall be clearly identified as a correction or addition to the original and shall be dated and initialed by the physician or other person who made the initial entry.

5. Requests for Amendment where our Practice was not the Originator of the Information

A. If a request for amendment applies to information for which our Practice was not the originator, our Privacy Officer will contact the requestor and advise the requestor to seek amendment from the originator of the information.

B. If the requestor notifies us of a reasonable basis to believe that the originator is no longer available to act on a requested amendment, our Privacy Officer shall make a reasonable attempt to confirm the unavailability. If the originator's unavailability is confirmed, our Practice will act on the request for amendment as though our Practice created the information.

6. Amendments Received from Other Covered Entities

A. If we are informed by another health care provider, a health care plan or a health care clearinghouse of an amendment to a patient's PHI, we will amend the patient's PHI that we maintain, accordingly.

B. The Privacy Officer shall:

i. Document in the patient's record that the approved amendment has been received from another source and the identity of the source providing the amendment;

ii. Ensure that the amendment is properly made in the PHI that is held by our Practice; and

iii. If the patient whose PHI is amended is a current patient of our Practice, alert the treating physician(s) for that patient of the amendment that has been made.

BUSINESS ASSOCIATES

Policy Number 9
HIPAA §§164.103, 502(e), 504(e), 532(d) & (e)

Policy: Before our Practice can disclose PHI to a Business Associate, or allow a Business Associate to create, receive, maintain or transmit PHI on our behalf, we will obtain satisfactory assurances that the Business Associate will use or disclose the PHI only as permitted or required by our Business Associate Agreement, will safeguard the PHI from misuse, will help the Practice comply with its duties under HIPAA and the Data Breach Notification Rule, and will secure these same assurances from any Subcontractor of the Business Associate. The Business Associate cannot use or disclose PHI provided by us in any manner that would not be a permissible use or disclosure by our Practice under the Privacy Rule.

Procedure:

1. Business Associates; Business Associate Agreements

   A. For each new arrangement where the Practice plans to retain a person or entity to perform a function, activity or service on behalf of the Practice, our Privacy Officer will first consult the definition of Business Associate in the Glossary of Terms to determine whether the person or entity is to be treated as a Business Associate of the Practice.

   B. Our Practice will enter into a written Business Associate Agreement with every person or entity who meets the definition of a Business Associate as set forth in the Glossary. Our Privacy Officer will consult our form of Business Associate Agreement and contact our legal counsel, as necessary, to assist in negotiation and/or preparation of the necessary agreement. Any Business Associate Agreement our Practice enters into shall meet the requirements of 45 C.F.R. §164.504(e)(1).

   C. If a Business Associate presents to our Practice the Business Associate's own proposed Business Associate Agreement, our Privacy Officer will review the proposed agreement under our model form and contact our legal counsel, as necessary, to assist in negotiation of necessary revisions to the proposed agreement(s).

   D. If our Practice has a Business Associate Agreement with an existing Business Associate Agreement that does not address requirements under the Data Breach Notification Rule or is not in compliance with the HITECH Act, we will enter into an Amended and Restated Business Associate Agreement and contact our legal counsel, as necessary, for assistance.

2. Confidentiality Agreements

Where the Privacy Officer has identified that a person or entity is not a Business Associate but, nevertheless, may have more than incidental or inadvertent access or exposure to PHI held by the Practice, the Privacy Officer will seek to enter into a confidentiality agreement with that person or entity and will obtain the advice of our legal counsel, as necessary.

3. Responding to Violations by a Business Associate

A. If any person in our Practice receives any information leading him or her to believe that one of our Business Associates (or an employee or agent of one of our Business Associates) is violating a provision of our Business Associate Agreement or is engaged in some activity that could result in a violation of our privacy policies and procedures, that person shall immediately provide that information to our Privacy Officer.

B. Our Privacy Officer shall keep a record of information provided to him or her pursuant to subsection 3A. If the information provided appears credible, the Privacy Officer shall contact the Business Associate to discuss the problem or may contact our legal counsel prior to contacting the Business Associate.

C. If the information received by the Privacy Officer reflects a pattern of activity or practice of the Business Associate that constitutes a material breach or violation of the Business Associate's obligations under our agreement with that entity or person, the Privacy Officer shall notify legal counsel for further action as required by the Privacy Rule.

SAFEGUARDING PROTECTED HEALTH INFORMATION

Policy Number 10
HIPAA §164.530(c)

Policy: Our Practice will have in place appropriate administrative, technical, and physical safeguards to try to reasonably safeguard our patients' PHI.

Procedure:

1. Our Practice will implement safeguards to reasonably:

    A. Protect our patients' PHI from intentional or unintentional use or disclosure in violation of the Privacy Rule and our policies and procedures; and

    B. Limit incidental uses or disclosures that may occur as a result of an otherwise permitted or required use or disclosure of PHI.

2. In determining what type of safeguards we should implement, we will take into consideration our own needs and circumstances, such as:

    A. The nature of the PHI we hold;

    B. The potential risks to patients' privacy;

    C. The potential effects on patient care; and

    D. The financial and administrative burden of implementing particular safeguards.

3. Some of the types of safeguards that our Practice will implement include:

    A. Development, implementation, and periodic review and revision of the policies and procedures in this Policy Manual;

    B. The designation of our Privacy Officer as the person responsible for implementing our policies and procedures, receiving complaints, and, along with his or her designee, providing information regarding our Notice of Privacy Practices;

    C. Proper storage and disposal of documents and records, such as shredding documents and records prior to disposal;

    D. Speaking quietly when discussing a patient's condition with family members in a

waiting room or other public area;

E. Avoiding use of patients' names in public hallways and other public areas of our office;

F. In areas where multiple patient-staff communications routinely occur, use of cubicles, dividers, shields, curtains, or similar barriers as is reasonable for our Practice;

G. Posting signs to remind employees to protect patient confidentiality;

H. Utilizing a patient sign-in sheet that does not include any of a patient's health information and, when calling out patient names or addressing patients in the waiting area, limiting the information disclosed, such as referring the patients to a reception area where they can receive further instructions in a more confidential manner;

I. Eliminating the posting of PHI in public areas where unauthorized persons can view the information;

J. Isolating or locking file cabinets or records rooms, or otherwise restricting medical records from access by unauthorized persons, such as maintaining reasonable supervision of these areas;

K. When maintaining patient charts outside of exam rooms, using such measures as reasonably limit access to these areas, such as ensuring that the area is supervised, escorting non-employees in the area, and/or placing patient charts in their holders with identifying information facing the door or wall or otherwise covered, rather than having health information about the patient visible to anyone who walks by;

L. Determining which Workforce members have access to keys and/or combinations to gain access to our office and/or to areas housing PHI and limiting such access to those whose duties require this level of access;

M. Imposing security measures on computers and other systems containing PHI, such as restrictions on workstation use, unique user ID's and strong passwords to access such computers, and firewalls;

N. Limiting visual access to computer monitors to avoid incidental disclosure of information to unauthorized persons, and utilizing automatic screen-savers with password re-entry or automatic log-off;

O. Establishing a disaster recovery plan, both for paper and electronic records;

P. Establishing a reporting and response system for security violations, in

conjunction with our Practice's Data Breach Notification Policy; and

Q. Providing periodic security awareness training to our Workforce.

TRAINING

Policy Number 11
HIPAA §164.530(b)

Policy: Our Practice will provide training to all Workforce members on the policies and procedures in this Policy Manual, as necessary and appropriate for them to carry out their function and duties within our Practice.

Procedure:

1. Our Privacy Officer shall develop and implement a training program for our Workforce to include the following:

    A. Making a copy of this Policy Manual available to all Members of our Workforce for the purpose of reviewing each policy and procedure (such review to occur in a training meeting(s) of our entire Workforce and/or through individual review by each member of our Workforce) or for consulting our policies and procedures on an as-needed basis;

    B. Informal awareness training regarding privacy and security of PHI, including application of the minimum necessary principle (see Policy No. 4 of this Policy Manual);

    C. Periodic reminders about the need to make good faith efforts to maintain the privacy and security of our patients' PHI;

    D. Education concerning computer virus protection, detection, and response to a virus infection; and

    E. Education about the importance of a secure login and our Practice's policy regarding creating, changing, and protecting the confidentiality of computer passwords.

2. Our Practice will provide this training as follows:

    A. To each member of our current Workforce;

    B. To each new member of our Workforce within a reasonable period of time after the person joins our Practice; and

    C. To each member of our Workforce whose job functions are affected by a material change in our policies or procedures or a material change in the HIPAA Privacy Rule, with such training to occur within a reasonable period of time after the material change becomes effective.

3. All Members of our Workforce shall:

   A. Sign a log indicating the date and content of training received by such person; and

   B. Sign a confidentiality agreement stating that the person has reviewed and understands the Practice's privacy policies and procedures and will strive to comply with them, and to reinforce each person's responsibility to protect and maintain the privacy and security of our patients' PHI.

4. Our Privacy Officer shall maintain records documenting that the training required by this policy is provided.

COMPLAINTS TO OUR PRACTICE; MITIGATION

Policy Number 12
HIPAA §164.530(d), (f)

Policy: Our Practice will provide a procedure for patients to make a complaint concerning our Practice's privacy policies and procedures or our Practice's compliance with such policies and procedures or with the HIPAA Privacy Rule.

Procedure:

1. A patient of our Practice who has a complaint about our policies and procedures regarding the handling of PHI, about our compliance with such policies and procedures or with the Privacy Rule, may file a complaint with our Privacy Officer.

    A. A complaint must be in writing and must state the specific nature of the problem with our policies and procedures or the specific area of alleged non-compliance.

    B. Our Privacy Officer will acknowledge to the patient, in writing, that we received the complaint and that it will be addressed appropriately and a response provided to the patient.

2. As specified in our Notice of Privacy Practices, a patient may also file a complaint directly with the Office for Civil Rights (see Glossary). The address for filing a complaint with the OCR will be provided to any person, upon request.

3. A complaint to our Practice shall be acted upon as soon as reasonably possible but in no case less than thirty (30) days of receipt.

4. Upon receipt of a complaint, our Privacy Officer shall advise the managing physician of our Practice, and, upon such review of the complaint, may notify our legal counsel for retention in reviewing, investigating, and formulating a response to the complaint.

5. Once the investigation into the complaint has been concluded, our Privacy Officer, in conjunction with legal counsel, shall formulate an appropriate response to the complaining individual.

6. If the investigation of the complaint revealed a problem with our policies and procedures, or a failure to comply with such policies and procedures or with applicable law or regulations, our Privacy Officer, in conjunction with our legal counsel, shall formulate corrective action intended to remedy the problem or non-compliance including, as appropriate, imposing sanctions pursuant to Policy No. 14 of this Manual.

7. If the violation is found to involve a Business Associate of our Practice, we shall take the

steps required by Policy No. 9 of this Policy Manual, regarding our Practice's Business Associates.

8. Our Privacy Officer shall document all complaints received and their disposition.

9. Any correspondence or communication our Practice receives from the OCR--whether regarding the investigation of a complaint, a compliance review, or otherwise--shall be immediately provided to our Privacy Officer who shall notify legal counsel for the Practice to assist in responding to the OCR. Our Practice shall cooperate with the OCR and provide access as required by the Privacy Rule.

10. Mitigation.

    A. Our Privacy Officer shall take reasonable efforts to mitigate, to the extent practicable, any harmful effect that is actually known to our Practice of a use or disclosure of PHI by our Practice or by one of our Business Associates, in violation of our policies and procedures or the requirements of law. Our Privacy Officer shall implement our Data Breach Notification Policy, to determine if any notice is required and what mitigation efforts should be undertaken

NO RETALIATION FOR THE EXERCISE OF RIGHTS OR THE FILING OF A COMPLAINT; NO WAIVER OF RIGHTS

Policy Number 13
HIPAA §164.530(g), (h)

Policy: Our Practice will not intimidate, threaten, coerce, discriminate against or take other retaliatory action against any individual who exercises, or attempts to exercise, his or her rights under the HIPAA Privacy Rule or who files a complaint or otherwise participates in HIPAA compliance efforts as described in this policy. Our Practice shall not require an individual to waive his or her rights under the HIPAA Privacy Rule as a condition of receiving treatment from our Practice.

Procedure:

1. All requests for access, amendment, copying, authorizations, acknowledgments, and accountings related to the PHI of a patient of our Practice shall be handled in accordance with this Policy Manual.

2. All complaints about our policies and procedures, or about our compliance with this Policy Manual, will be handled in accordance with this Policy Manual and no patient, Personal Representative, or Member of our Workforce will be retaliated against in any way for:

    A. Filing a complaint with our Privacy Officer or with the Secretary of Health and Human Services (Office for Civil Rights) pursuant to Policy No. 12 of this Policy Manual;

    B. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing related to the Privacy Rule; or

    C. Opposing any act or practice that is unlawful under the HIPAA Privacy Rule, provided the person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI made in violation of the HIPAA Privacy Rule.

3. Workforce members are encouraged to contact our Privacy Officer for clarification in the event of confusion or questions concerning any part of this Policy Manual.

4. Workforce members are encouraged to and shall immediately report, in good faith, to our Privacy Officer, or to our managing physician, any knowledge of a violation of this Policy Manual by a member of our workforce or by a Business Associate, or a violation of this policy of non-retaliation and non-waiver of rights.

5. If our Practice receives information that this policy may have been violated, our Privacy Officer, or managing physician, as appropriate to the complaint, shall promptly investigate the report of retaliation and shall consult with our Practice's legal counsel regarding the matter, as necessary.

6. Any Member of our Workforce found to have violated this policy shall be sanctioned according to the provisions of Policy No. 14 of this Manual and consistent with our personnel policies.

SANCTIONS FOR VIOLATIONS OF PRIVACY; EXCEPTIONS TO SANCTIONS

Policy Number 14
HIPAA §164.530(e), (g)(2); §164.502(j)

Policy: Our Practice will apply appropriate sanctions against any member of our Workforce who fails to comply with the policies and procedures in this Policy Manual or the requirements of the Privacy Rule. Sanctions will not be imposed, however, under certain circumstances described in this Policy.

Procedure:

1. General Sanction Policy

   A. Our Practice may receive complaints regarding our compliance with our Policies and Procedures or with the Privacy Rule. Such complaints will be handled in accordance with Policy No. 12 of this Manual. We may also learn of non-compliance issues through allegations of violations received internally from our Workforce members.

   B. Workforce members are encouraged to make our Privacy Officer or managing physician aware of any concerns about our compliance with our Privacy Policies or with the Privacy Rule. Any allegations of noncompliance should be made in good faith, and in accordance with this policy, as applicable.

   C. All allegations of a violation by a member of our Workforce of a provision of this Policy Manual will be investigated. Appropriate disciplinary action will be taken whenever it is determined that a member of our Workforce has committed a significant violation of our Policy Manual or the Privacy Rule. The established disciplinary procedures and processes are applicable to all Workforce members, whether an owner, employee or independent contractor.

   D. The determination of the disciplinary measures to be imposed will be made on a case-specific basis, appropriate to the nature of the violation, and in accordance with our personnel policies. We will consider factors such as:

      i. The severity of the violation;

      ii. Whether it was intentional or unintentional; and

      iii. Whether there has been a pattern of noncompliance by the member of our Workforce.

E. Disciplinary actions may include counseling, verbal warning, written warning, suspension without pay, and/or discharge.

F. As set forth in Policy No. 11 of this Manual, we will have procedures in place requiring our Workforce members to review and become familiar with our privacy policies and procedures so they will understand what is expected of them in the area of privacy and be aware that noncompliance could result in sanctions. Such training will include the specific requirements set forth in Section 2, below, regarding otherwise impermissible disclosures.

G. Our Privacy Officer will be responsible for documenting all sanctions and disciplinary action resulting from a violation.

2. Exceptions to Sanctions

Sanctions shall not apply to a member of our Workforce with respect to the following activities, where the specific requirements for each type of activity or disclosure is met:

A. Actions taken in pursuit of compliance with the Privacy Rule

Our Practice will not intimidate, threaten, coerce, discriminate against or take other retaliatory action against Workforce members or others who:

i. File a complaint with the Secretary of Health & Human Services, or the Office for Civil Rights;

ii. Testify, assist or participate in an investigation or a compliance review, proceeding or hearing related to OCR's enforcement of the Privacy Rule;

iii. Oppose any act or practice made unlawful by the Privacy Rule, provided the person has a good faith belief that the act or Practice is unlawful, and the manner of the opposition is reasonable and does not involve disclosures of PHI in violation of the Privacy Rule.

B. Whistleblowers

Our Practice will not impose sanctions or otherwise retaliate against a member of our Workforce or a Business Associate of our Practice who discloses PHI in the following circumstances:

i. The individual believes that the conduct at issue (which requires the disclosure of PHI in order for the individual to report the conduct) is unlawful or otherwise violates professional or clinical standards, or that the care, services or conditions provided by our Practice potentially endangers one or more patients, workers or the public and if;

ii. The disclosure is made to one of the following:

a. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of our Practice;

b. An appropriate health care accreditation organization for the purpose of reporting the allegation of misconduct or failure to meet professional standards or misconduct by our Practice; or

c. An attorney retained by or on behalf of the member of our Workforce or Business Associate for the purpose of determining the person's legal options and/or obligations with regard to the Practice's conduct.

C. Victims of Crime

Our Practice will not impose sanctions or otherwise retaliate against a member of our Workforce who is the victim of a criminal act and discloses PHI related to the crime, provided that:

i. The disclosure is to a law enforcement official;

ii. The PHI disclosed is about the suspected perpetrator of the criminal act; and

iii. The PHI disclosed is limited to the following information:

a. Name and address;
b. Date and place of birth;
c. Social security number;
d. ABO blood type and Rh factor;
e. Type of injury;
f. Date and time of treatment;
g. Date and time of death, if applicable; and
h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos.

GLOSSARY OF TERMS

Authorization - The permission granted by a patient, or the patient's Personal Representative, to use Protected Health Information for specified purposes or to disclose Protected Health Information to a third party specified by the individual. An *Authorization Form* is the document that reflects this permission.

Breach - With certain exceptions, the acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI.

Business Associate - With certain exceptions, a person or entity that: (1) creates, receives, maintains, or transmits PHI for a function or activity regulated by the Privacy Rule or (2) provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for our practice, or to or for an Organized Health Care Arrangement in which our practice participates, where the provision of the service involves the disclosure of protected health information from our practice or OCHA, or from our Business Associate, to the person. A Business Associate does not include a member of the Covered Entity's Workforce nor a health care provider with respect to disclosures by the Covered Entity to the health care provider concerning the treatment of a patient. A Business Associate includes: a personal health record vendor, Health Information Organization, and an E-prescribing Gateway or other organization that provides data transmission of PHI to a Covered Entity and requires access to such PHI on a routine basis but not organizations that are mere conduits for the transport of PHI and do not access the information other than on a random or infrequent basis. A Business Associate is also a subcontractor that creates, receives, maintains or transmits PHI on behalf of a Business Associate.

Business Associate Agreement - A Covered Entity's written agreement with its Business Associate, setting forth the Business Associate's obligations related to the Covered Entity's PHI.

Correctional Institution - Any penal or correctional facility, jail, reformatory, detention Practice, work farm, halfway house, or residential community program Practice operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons* held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses or others awaiting charges or trial. *Inmate* is a person incarcerated in or otherwise confined to a correctional institution. *Covered Entity* - A health care provider who conducts certain financial and administrative transactions electronically for which standards have been adopted under HIPAA, such as electronic billing. Health Plans and Healthcare Clearinghouses are also Covered Entities.

Data Breach – See our Practice's Data Breach Notification Policy.

Designated Record Set - Basically a group of records which a Covered Entity uses to make decisions about individuals, and includes a health care provider's medical records and billing records, and a health plan's enrollment, payment, claims adjudication, and case or medical management record systems. A *record,* for purposes of a Designated Record Set, means any item, collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for a Covered Entity.

Direct Treatment Relationship - A treatment relationship between an individual and a health care provider that is not an Indirect Treatment Relationship.

Disclosure - The release, transfer, provision of access to, or divulging in any other manner, of information outside the entity holding the information.

Electronic Health Record – An electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

Electronic Media - (1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.
Electronic Protected Health Information (EPHI) -

Family Member - An individual's: (1) dependent; or (2) any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents). First-degree relatives include parents, spouses, siblings, and children. Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces. Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins. Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

Health Care – Health care includes, but is not limited to, the following: Preventive, diagnostic, therapeutic, rehabilitative maintenance, or palliative care, and counseling service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health Care Clearinghouse - A public or private entity that either: (1) processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; or (2) receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health Care Operations - Certain administrative, financial, legal, and quality improvement activities of a Covered Entity that are necessary to run its business and to support the core functions of treatment and payment. These activities are limited to the activities listed in the definition of "health care operations" at 45 CFR 164.501, such as : conducting quality assessment and improvement activities and case management and care coordination; reviewing the competence or qualifications of health care professionals, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities; conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs; business planning and development; and business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other HIPAA rules, customer service, resolution of internal grievances, sale or transfer of assets, and creating de-identified health information or a Limited Data Set.

Health Information - Any information, including genetic information, whether oral or recorded in any form or medium, created or received by a provider that relates to the past, present, or future physical or mental health condition of a patient; the provision of healthcare to a patient; or the past, present or future payment for the provision of healthcare to a patient.

Health Oversight Agency - An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Health Plan - An individual or group plan that provides for, or pays the cost of, medical care.

HHS - The U.S. Department of Health & Senior Services (see *Secretary*).

HIPAA - The Health Insurance Portability and Accountability Act of 1996.

HITECH – The Health Information Technology for Economic and Clinical Health Act.

Incidental use or disclosure - A secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of a use or disclosure permitted by the Privacy Rule.

Indirect Treatment Relationship - A relationship between an individual and a health care

provider in which: (1) the health care provider delivers health care to the individual based on the orders of another health care provider; and (2) the health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

Individual - The person who is the subject of Protected Health Information.

Institutional Review Board or *IRB* or *Privacy Board* - Within the provisions of the institutional review board (IRB) rules (21 CFR, Part 56) are requirements that the IRB ensure that there are adequate provisions to protect the privacy of research subjects and to maintain the confidentiality of research data.

Law Enforcement Official - An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to: (1) investigate or conduct an official inquiry into a potential violation of law; or (2) prosecute or otherwise conduct a criminal, civil or administrative proceeding arising from an alleged violation of law.

Limited Data Set – A Limited Data Set is PHI that excludes the following direct identifiers of the individual or of relatives, employers or household members of the individual:

- Names;
- Postal address information, other than town or city, State, and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

Marketing - Marketing means:

(1) (except as provided in (2) below) to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(2) Marketing <u>does not</u> include a communication made:

(i) to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the Covered Entity in exchange for making the communication is reasonably related to the Covered Entity's cost of making the communication;

(ii) for the following treatment and health care operations purposes, except where the Covered Entity receives financial remuneration in exchange for making the communication: (A) for treatment of an individual by a health care provider including: case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or setting of care to the individual; (B) to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the Covered Entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health0related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or (C) for case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

(3) Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

Minimum Necessary - The principle that a Covered Entity, when using or disclosing PHI, or when requesting PHI from another Covered Entity, must make reasonable efforts to limit such PHI, to the extent practicable, to the *Limited Data Set* or, if needed by the Covered Entity, to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. The Secretary of HHS will issue guidance on what constitutes "minimum necessary."

OCR - The Office for Civil Rights of the U.S. Department of Health & Human Services. OCR is the federal agency charged with enforcing the Privacy Rule and receives complaints regarding same. The OCR address for filing complaints related to our Practice is the Region II – New York OCR Office (New Jersey, New York, Puerto Rico, Virgin Islands):

Linda Colon, Regional Manager
Office for Civil Rights
U.S. Department of Health and Human Services
Jacob Javits Federal Building
26 Federal Plaza - Suite 3312
New York, NY 10278
Voice Phone (800) 368-1019
FAX (212) 264-3039
TDD (800) 537-7697

Organized Health Care Arrangement (OHCA) - An Organized Health Care Arrangement is: (1) a

clinically integrated care setting in which individuals typically receive health care from more than one health care provider; or (2) an organized system of health care in which more than one Covered Entity participates, and in which the participating Covered Entities: (i) hold themselves out to the public as participating in a joint arrangement; and (ii) participate in joint activities that include at least one of the following: (A) utilization review, in which health care decisions by participating Covered Entities are reviewed by other participating Covered Entities or by a third party on their behalf; (B) quality assessment and improvement activities, in which treatment provided by participating Covered Entities is assessed by other participating Covered Entities or by a third party on their behalf; or (C) payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating Covered Entities through the joint arrangement and if PHI created or received by a Covered Entity is reviewed by other participating Covered Entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

Payment - The various activities of health care providers to obtain payment or be reimbursed for their services and of a Health Plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care. It includes billing and collection activities, determining eligibility or coverage under a plan and adjudicating claims, reviewing health care services for medical necessity, coverage, justification of charges, etc., utilization review activities (including precertification and preauthorization of services, concurrent and retrospective review of services), and disclosures to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: name and address; date of birth; social security number; payment history; account number; and name and address of the health care provider and/or Health Plan.

Personal Representative - Under the Privacy Rule, a person authorized under State or other applicable law to act on behalf of the individual in making health care related decisions is the individual's personal representative. Except in certain limited situations specified in the Privacy Rule, a Covered Entity is required to treat an individual's Personal Representative as the individual with respect to uses and disclosures of the individual's PHI, as well as with respect to the individual's rights under the Privacy Rule. *PHI* - Protected Health Information. Protected Health Information is individually identifiable health information that is: (i) transmitted by electronic media; (ii) maintained in any electronic medium; or (iii) transmitted or maintained in any other form or medium, but does not include certain education records covered by the Family Educational Rights and Privacy Act or employment records held by a Covered Entity in its role as an employer. A Covered Entity need only comply with the requirements of the Privacy Rule with respect to the PHI of a deceased individual for a period of 50 years following the death of the individual.

Privacy Act means the Privacy Act of 1974 (5 U.S.C., section 552A).

Privacy Contact - The person or persons designated by our Practice to answer questions and provide information to patients and others about our Notice of Privacy Practices and our policies and procedures, if this role is not filled by our Privacy Officer.

Privacy Rule - The Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164.

Privacy Officer - The person designated by our Practice to oversee the development and implementation of our Practice's privacy policies and procedures and, where not delegated to a Privacy Contact(s), the person who receives complaints about our privacy practices and answers questions about our Notice of Privacy Practices.

Psychotherapy Notes - Notes recorded (in any medium) by a health care provider who is 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 separated from the rest of the individual's medical record. It 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: diagnoses, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Public Health Authority - An agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. Examples of a public health authority include State and local health departments, the Food and Drug Administration (FDA), the Centers for Disease Control and Prevention (CDC), and the Occupational Safety and Health Administration (OSHA).

Required by Law - A mandate contained in law that compels a Covered Entity to make a use or disclosure of PHI and that is enforceable in a court of law, e.g., court orders, court-ordered warrants, subpoenas, and summons; a civil investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Research - A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Sale of PHI – With certain exceptions set forth at 45 CFR §164.502(a)(5)(ii)(B)(2), a disclosure of PHI by a Covered Entity or Business Associate, if applicable, where the Covered Entity or Business Associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

Secretary - The Secretary of the U.S. Department of Health & Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Subcontractor – A person to whom a Business Associate delegates a function, activity or service, other than in the capacity of a member of the Workforce of such Business Associate.

Treatment - The provision, coordination or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient, from one health care provider to another, for health care.

Use - With respect to Individually Identifiable Health Information, is the sharing, employment, application, utilization, examination or analysis of such information within an entity that maintains such information.

Workforce - Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity or Business Associate, is under the direct control of such Covered Entity or Business Associate, whether or not they are paid by the Covered Entity or Business Associate.