MODEL POLICIES AND PROCEDURES
OF

_____

The following policies and procedures are intended to comply with the federal Health Insurance Portability and Accountability Act of 1996, the federal Health Information Technology for Economic and Clinical Health Act and all related regulations.

For the purposes of this document, the following definitions apply:

"HIPAA Rules" shall mean the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR Part 160 and Part 164.

The following terms used in this document shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information or PHI, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured PHI and Use.

I. NOTICE OF PRIVACY PRACTICES

We will prepare and provide to all patients a document called a Notice of Privacy Practices ("Notice"). This Notice will detail our policies and procedures with respect to the handling of confidential patient information and in the event of a breach of information. The Notice also will set forth detailed information about patients' individual rights with respect to their own health information.

We will provide a copy of the Notice to all patients and ask each patient to acknowledge receipt of the Notice by signing an acknowledgment form. The patient is NOT required to sign the acknowledgment form but we will make a reasonable effort to obtain an acknowledgment from each patient we see. If after reasonable efforts, such acknowledgment cannot be obtained, we will make a note of this in the patient's file. In emergency situations, we may defer giving the Notice and obtaining an acknowledgment until the patient's medical condition permits. Patient refusal to acknowledge receipt of the Notice is NOT a bar to treatment.

All new patients will receive a copy of the Notice at the first office visit. In addition, the Notice will be made available to any person who asks for it. If we revise or update the Notice with a material change, we will re-distribute the Notice to all patients. If the revision or update is non-material, we will provide the new Notice to all new patients at the first date of service and to current patients only upon request. In addition, we will post our Notice and any revised versions in a prominent location in our medical offices and on our website if we maintain one. We will not use or disclose patient health information in a manner inconsistent with the Notice.

II. DESIGNATION OF PRIVACY OFFICER

We will designate a privacy officer who is responsible for the development and implementation of our policies and procedures and we will document who has been designated as our privacy officer.

Name of Privacy Officer: _____

III. USES AND DISCLOSURES OF HEALTH INFORMATION

Federal law permits us to use and disclose personal health information without consent or authorization for purposes of treatment, payment, and health care operations. However, under New York State law and regulations, we will not release personal health information to any third party except in the following circumstances:

1. With the Patient's Express Consent for Treatment and Payment

   This consent may be in writing, oral or implied.

   Examples:

   - A patient sends us a written request to send a copy of his or her records to another physician who may be providing treatment to the patient.
   - A patient asks that we call the pharmacy to renew their medication.
   - A patient asks that we submit a health insurance claim form to the patient's insurance carrier or the patient seeks treatment from us because we are a participating provider in the patient's health plan.

2. As Otherwise Permitted or Required by Federal or State Law or Regulation

   Examples:

   - In an emergency situation
   - For child abuse and neglect reporting and investigation

3. For Our Internal Operations

   We will share information among our employees, including students and trainees, and consultants to perform the operations of our medical office, such as billing and record keeping. We will share with our employees and business associates only the minimum amount of personal health information necessary for them to assist us.

4. Pursuant to Written Authorization From the Patient

   In connection with any other uses and disclosures not described in this Notice, we will not release health information to any third party unless the patient grants us written authorization to do so.

   Examples:

   - We receive a request for medical information from a patient's prospective employer
   - In connection with use or disclosure of psychotherapy notes
   - In connection with marketing activities
   - In connection with the sale of protected health information

IV. OTHER USES AND DISCLOSURES

In addition to uses and disclosures related to treatment, payment, and health care operations, we may also use and disclose personal health information without the patient's express consent or authorization for the following additional purposes:

Abuse, Neglect, or Domestic Violence
As required or permitted by law, we may disclose health information to a state or federal agency to report suspected abuse, neglect, or domestic violence. If such a report is optional, we will use our professional judgment in deciding whether or not to make such a report. If feasible, we will promptly inform the patient that we have made such a disclosure.

Appointment Reminders and Other Health Services
We may use or disclose health information to remind a patient about appointments or to inform the patient about treatment alternatives or other health-related benefits and services that may be of interest, such as case management or care coordination.

Business Associates
We may share health information with business associates who are performing services on our behalf. For example, we may contract with a company to do our billing. Our business associates are obligated to safeguard all health information they receive. We will share with our business associates only the minimum amount of health information necessary for them to assist us.

Communicable Diseases
To the extent permitted or required by law, we may disclose information to a public health official or a person who may have been exposed to a communicable disease or who is otherwise at risk of spreading a disease or condition.

Communications with Family and Friends
We may disclose information to persons who are involved in a patient's care or payment for care, such as family members, relatives, or close personal friends. In addition, we may notify a family member, personal representative, or other person responsible for a patient's care, of the patient's location, general condition, or death. Any such disclosure will be limited to information directly related to the person's involvement in care. If the patient is available and has capacity, we will provide the patient with an opportunity to object before disclosing any such information. If the patient is unavailable because, for example, the patient is incapacitated or because of some other emergency circumstance, we will use our professional judgment to determine what is in the patient's best interest regarding any such disclosure.

Coroners, Medical Examiners and Funeral Directors
In the event of a patient's death, we may disclose health information to a coroner or medical examiner, for example, to assist in identification or determining cause of death. We may also disclose health information to funeral directors to enable them to carry out their duties.

Disaster Relief
We may disclose health information to government entities or private organizations (such as the Red Cross) to assist in disaster relief efforts. If the patient is available, we will provide the patient with an opportunity to object before disclosing any such information. If the patient is unavailable because, for example, the patient is incapacitated, we will use our professional judgment to determine what is in the patient's best interest and whether a disclosure may be necessary to ensure an adequate response to the emergency circumstances.

Food and Drug Administration (FDA)
We may disclose health information to the FDA, or to an entity regulated by the FDA, for example, in order to report an adverse event or a defect related to a drug or medical device.

Health Oversight
We may disclose health information for oversight activities that are authorized by federal or state law, for example, to facilitate auditing, inspection, or investigation related to our provision of health care, or to the health care system.

Judicial or Administrative Proceedings
We may disclose health information pursuant to a court order in connection with a judicial or administrative proceeding, in accordance with our legal obligations

Law Enforcement
We may disclose health information to a law enforcement official for certain law enforcement purposes without the consent of the patient but only when the patient is incapacitated or in an emergency situation.

Minors
If the patient is an unemancipated minor under New York law, there may be circumstances in which we disclose health information about the patient to a parent, guardian, or other person acting *in loco parentis*, in accordance with our legal and ethical responsibilities.

Parents
With respect to the parent of an unemancipated minor acting as the minor's personal representative, we may disclose health information about the child to the parent under certain circumstances. For example, if we are legally required to obtain the parent's consent (if the parent is the child's personal representative) in order for the child to receive care from us, we may disclose health information about the child to the parent. In some circumstances, we may not disclose health information about an unemancipated minor to the parent. For example, if the child is legally authorized to consent to treatment (without separate consent from a parent or personal representative), consents to such treatment, and does not request that the parent be treated as his or her personal representative, we may not disclose health information about the child to the parent without the child's written authorization.

Personal Representative
If the patient is an adult or emancipated minor, we may disclose health information to a personal representative authorized to act on behalf of the patient in making decisions related to health care.

Public Health Activities
As required or permitted by law, we may disclose health information to a public health authority, for example, to report disease injury or vital events such as death.

Public Safety
Consistent with our legal and ethical obligations, we may disclose health information to law enforcement or to potential victims based on a good faith determination that such disclosure is necessary to prevent a serious and imminent threat to the patient or others.

Required By Law
We may disclose health information as required by federal, state or other applicable law.

Specialized Government Functions
We may disclose health information for certain specialized government functions, as authorized by law and depending on the particular circumstances. Examples of specialized government functions include military activities, determination of veterans benefits and emergency situations involving the health, safety, and security of public officials.

Workers' Compensation
We may disclose health information for purpose related to workers' compensation, as required and authorized by law.

V. AUTHORIZATION

We will obtain an Authorization from the patient for all non-routine uses and disclosures of patient health information. An example of a non-routine use or disclosure is the release of information in connection with a pre-employment medical evaluation, release of psychotherapy notes, marketing communications or the sale of PHI. An Authorization is a written document that must be prepared on a case-by-case basis and signed by the patient. The Authorization must contain specific and detailed information about the type of health information to be disclosed, to whom it is to be disclosed and must contain an expiration date or event. The patient may revoke the Authorization at any time, except when we have taken action in reliance upon the Authorization. The Authorization form must be filled out completely and must be signed by the patient in order to be valid. We will maintain a form of Authorization to be used in all appropriate situations. A signed Authorization sent by facsimile is acceptable. A copy of the Authorization will be provided to the patient and the original maintained in the patient's file.

We are not permitted to condition the provision of treatment on the provision of an Authorization, except in the case of research-related treatment or the provision of health care solely for the purpose of creating PHI for disclosure to a third party, such as in the case of pre-employment medical assessments.

VI. MINIMUM NECESSARY RULE

When using, disclosing or requesting protected health information, we will access only the minimum necessary amount of information. The term minimum necessary means the least amount of information required to achieve the purpose of the use, disclosure or request. Access to information by any office staff or service providers must be limited to that information necessary to accomplish the task at hand.

The minimum necessary rule does not apply in the following circumstances:

- in the course of treating a patient;
- uses or disclosures made pursuant to a valid authorization;
- uses or disclosures made to the individual;
- disclosures to the Secretary of the Department of Health and Human Services;
- uses or disclosures that are required by law; and
- uses or disclosures required to comply with the Privacy Rule.

If we have employees in our office, we will identify which persons in our workforce need access to PHI to carry out their duties and identify the categories of PHI to which access is needed. We will make reasonable efforts to limit such access to the amount and type of PHI required for the particular use or disclosure.

For routine and recurring disclosures of or requests for PHI, we will establish procedures designed to limit the PHI disclosed to the minimum amount necessary. For non-routine disclosures, we will develop criteria designed to limit the PHI disclosed to the minimum amount necessary.

We will rely on a request for disclosure as being for the minimum necessary amount of information if: (i) the request is from a public official and the official represents that the request is for the minimum necessary information; (ii) the request is from another covered entity; or (iii) the request is from one of our business associates and the business associate represents that the request is for the minimum necessary information.

Incidental disclosures of health information, such the overhearing of a conversation, are not a violation of the Privacy Rule. We will not be held liable for incidental disclosures otherwise authorized by the rule as long as we take reasonable efforts to safeguard and maintain the confidentiality of personal health information.

VII. DE-IDENTIFIED INFORMATION

Any PHI that has been de-identified may be used or disclosed without violating the provisions of the Privacy Rule or these Policies and Procedures. Information is de-identified if:

(1) A person with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods determines that the risk is very small that the information could be used, alone or with other reasonably available information, to identify the individual who is the subject of the information; or

(2) (i) all of the following identifiers of the individual (and relatives, employers or household names) are removed:

a. names;
b. all geographic subdivisions smaller than a State;
c. elements of dates (except year) directly related to the individual, and all ages for individuals over 89, unless aggregated into a single category of age 90 and older;
d. telephone numbers, fax numbers, email addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate or license numbers, vehicle identifiers and serial numbers, including license plate numbers, device identifiers and serial numbers;
e. Web Universal Resource Locators (URLs);
f. Internet Protocol (IP) address numbers;
g. biometric identifiers;
h. full face photographic images; and
i. any other unique identifying number, characteristic or code (e.g. indictment numbers or docket numbers)

and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

VIII. BUSINESS ASSOCIATES

We will enter into a business associate agreement with all of our business partners and contractors who receive PHI as part of their duties. We will enter into the business associate agreement no later than April 14, 2003, with some exceptions. The business associate agreement will require business associates to appropriately safeguard any PHI they receive in the course of their work for us. The business associate agreement will contain all provisions required by the Privacy Rule. If our business associate violates the business associate agreement and any steps to cure the violation were unsuccessful, we will either immediately terminate the agreement or, if termination is infeasible, report the violation to HHS. A business associate agreement is NOT required in the case of disclosures by us to another health care provider for treatment purposes.

IX. VERIFICATION OF IDENTITY AND AUTHORITY

Except in emergency situations, and using reasonable efforts under the circumstances, we will verify the identity and the authority of any party requesting access to PHI, including obtaining any necessary documentation.

X. PERSONAL REPRESENTATIVES

We will treat any personal representative of an individual as if he or she is the individual. A personal representative is a person who has authority under applicable law to act on behalf of an adult or emancipated minor in making decisions related to health care. With respect to unemancipated minors, a personal representative is a parent, guardian or other person acting *in loco parentis* who has authority under applicable law to act on behalf of the unemancipated minor in making decisions related to health care. However, such person may not be the personal representative of an unemancipated minor and the minor may act as an individual if: (i) the minor consents to the health care service and no other consent is required by law; (ii) the minor may lawfully obtain such health care service without the consent of a parent or guardian, and the minor has consented to the service; or (iii) a parent or guardian assents to an agreement of confidentiality between the health care provider and the minor with respect to such health care service. We will treat an executor, administrator or other person who has the authority to act on behalf of a deceased individual or on behalf of the individual's estate as the personal representative of the individual.

XI. PATIENTS' RIGHTS

In order to exercise any of the patients' rights described below, the patient must submit a request in writing to our contact person or designated Privacy Officer. If patients have any questions about their rights, we will direct them to our Privacy Officer.

A. Right to Inspect or Copy Records

All patients have the right to review, or to receive a copy of, the health information maintained about them in our files and used to make decisions about their treatment. We ordinarily will provide the individual with an opportunity to inspect records no later than 10 days from the date of the request. We ordinarily will provide copies of records no later than 30 days from the date of the request for on-site records and 60 days from the date of the request for off-site records. The standard fee for copying is $0.75 per page. If we maintain an electronic health record for an individual, the individual may request access to the individual's health information in an electronic format or have the information transmitted electronically to a designated recipient. Any fee charged by us for the electronic document production cannot exceed our labor costs in responding to the request.

Under certain circumstances, we may deny an individual's request for access to their PHI. We may deny access for the following reasons *without an opportunity for review of such denial*:

- if the request is not made in writing
- request is for information compiled in connection with a legal proceeding
- request is for information subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA)
- if we obtained the requested information from someone other than a health care provider under a promise of confidentiality and such access would be reasonably likely to reveal the source of the information
- request is for information obtained in the course of research
- request is for information maintained by us acting under the direction of a correctional institution, and providing access to the PHI would jeopardize the health, safety, security, custody or rehabilitation of the individual or other persons at the institution

We may deny the individual's request for access to their PHI in the following circumstances, *but we are required to provide an opportunity for review of such denial*:

- if access would reasonably be expected to cause substantial harm to the individual or others which would outweigh the need for such access
- if access is likely to endanger the life or physical safety of the individual or another person
- if the information refers to a third person and access would likely cause harm to that third person

If we are unable to satisfy the patient's request for access, we may instead provide the patient with a summary of the information requested. We will inform the patient in writing of the reason for the denial and their right, if any, to request a review of the decision and how to do so.

B. Right to Amend Record

A patient may request that we amend the health information that is maintained in our files about them. The patient's request must explain why he or she believes that the records are incorrect or otherwise require amendment. Ordinarily, we will respond to a request for an amendment within 60 days. If we are unable to satisfy the request, we will inform the patient in writing of the reason for the denial and let them know how they may contest the decision, including a right to submit a statement (of reasonable length) disagreeing with the decision. This statement will be added to the patient's file.

C. Right to Request Restrictions

A patient may request that we restrict certain uses and disclosures of their health information. We are not, however, required to agree to all requested restrictions, unless the requested restriction involves information to be sent to a health plan for payment or health care operations purposes and the disclosure relates to products or services that were paid for in full by the patient and such disclosure is not otherwise required by law.

D. Right to Request Communications by Alternative Means

A patient may request that we communicate with them by alternative means, such as making records available for pick-up, or mailing them to an alternative address, such as a P.O. box. We will accommodate reasonable requests for such confidential communications.

E. Right to Receive an Accounting for Disclosures

A patient may request an accounting of all disclosures of their PHI. The accounting must include the following information: the date of the disclosure, the name of person or entity who received the information and their address if known, a brief description of the PHI disclosed and the reason for the disclosure.

Customarily, a patient is not entitled to receive an accounting when the disclosure was made under the following circumstances:

- to the individual
- for routine (i.e. treatment and payment) purposes
- for the internal operations of our medical office
- incident to an otherwise permitted or required use or disclosure
- pursuant to a valid authorization
- for notification purposes, such as to other individuals involved in the patient's health care
- for national security purposes
- to correctional institutions or law enforcement
- made prior to the Privacy Rule compliance date of April 14, 2003
- made more than six years prior to the request

However, if we maintain an electronic health record for a patient, the patient may be entitled to receive an accounting of routine disclosures only of any health information maintained in the electronic health record for the three year period prior to the date of the request.

We will respond to the patient's request for an accounting of disclosures within 60 days of the date of the request. If we are unable to meet the 60 day deadline, we may extend our response time by 30 days. If such an extension is required, we will inform the patient in writing of the reason for the delay. We will provide the patient with one accounting free of charge, however if they request more than one accounting in any 12 month period, we may impose a reasonable, cost-based fee for any subsequent request. We will ask the patient to tailor their request to a particular period of time (for example, "from May 1, 2013 to June 1, 2013"). We will be unable to provide an accounting for any disclosures made before April 14, 2003, or made more than six years ago.

F. Right to Request a Copy of our Notice of Privacy Practices

A patient has the right to request a paper copy of our Notice of Privacy Practices, or an electronic copy, if applicable.

XII. NOTICE OF BREACH OF HEALTH INFORMATION

Under HIPAA, an impermissible use, access or disclosure is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that PHI has been compromised based on a risk assessment of at least the following factors: (i) the nature and extent of the PHI involved; (ii) who gained access to the PHI; (iii) whether the PHI was actually acquired or viewed and (iv) the extent to which the risk to the PHI has been mitigated. If a breach occurs and we determine that notice is required, we will provide written notice to the individual affected as described below.

A. Notice to the Individual

The required notice will be sent without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. A breach will be treated as discovered by us as of the first day on which the breach is known to us or would have been known to a covered entity exercising reasonable diligence. The notice will be written in plain language and will contain the following information: (i) a brief description of what happened, the date of the breach, if known, and the date of discovery; (ii) the type of PHI involved in the breach; (iii) any precautionary steps the individual should take; (iv) a description of what we are doing to investigate and mitigate the breach and prevent future breaches; and (v) contact information for us, including a toll-free telephone number, e-mail address, website or postal address.

The notice will be sent by first-class mail or by email, if the individual has specified a preference for communication by email. If contact information for the individual in question is insufficient or out-of-date, we may contact the individual by telephone or other permissible alternate method of communication.

Finally, if the notification is of an urgent nature because of possible imminent misuse of unsecured health information, we may contact the individual by telephone or other means, as appropriate, in addition to the written or other forms of notice.

B. Notice to the Media

In the event of a breach affecting more than 500 residents of a State or jurisdiction, we will, without unreasonable delay and in no case later than 60 calendar days after discovery of the breach, notify prominent media outlets serving the State or jurisdiction.

C. Notice to HHS

For breaches affecting fewer than 500 individuals, we are required to maintain an annual log of such breaches and provide a copy of such log to HHS within 60 days of the end of the calendar year. For breaches affecting 500 or more individuals, we are required to notify HHS at the same time notice is provided to the individual.

D. Law Enforcement Delay

Following a breach, we may delay transmission of any of the required forms of notice if we are informed by a law enforcement official that such notice would impede a criminal investigation or cause damage to national security.

XIII. OTHER ADMINISTRATIVE REQUIREMENTS

A. Safeguards for Protected Health Information

We will implement administrative, technical and physical safeguards to reasonably protect the privacy of protected health information. We will safeguard PHI from intentional or unintentional disclosures in violation of the Privacy Rule and we will limit incidental uses or disclosures of PHI.

B. Training

If we have employees in our office, we will provide training to all members of our workforce about the Privacy Rule and these Policies and Procedures as necessary and appropriate for the members of the workforce to carry out their functions within the practice. If there is a material change in our policies or procedures, we will provide additional training to all workers whose functions would be affected by such a change. We will document all training provided.

C. Mitigation

We will mitigate, to the extent practicable, any harmful effect known to us of a use or disclosure made by us or by a business associate in violation of the Privacy Rule or our Policies and Procedures.

D. Sanctions

We will implement and impose sanctions on any member of our workforce who fails to comply with the Privacy Rule or these Policies and Procedures. We will document any such sanctions imposed.

E. Intimidating or Retaliatory Acts

We will refrain from intimidating, threatening, coercing, discriminating against, or taking retaliatory action against any individual for exercising his or her rights under the Privacy Rule or opposing any act or practice in violation of the Privacy Rule.

F. No Waiver of Rights

We will not require individuals to waive their rights under the Privacy Rule as a condition of treatment.

XIV. COMPLAINTS

If a patient believes his or her privacy rights have been violated, they may file a written complaint with us by mailing it or delivering it to our contact person. The patient also may complain to the Secretary of Health and Human Services (HHS) by writing to Office for Civil Rights, U.S. Department of Health and Human Services, 200 Independence Avenue, S.W., Room 509F, Washington, D.C. 20201; by calling 1-800-368-1019; or by sending an email to OCRprivacy@hhs.gov. We cannot, and will not, make patients waive their right to file a complaint with HHS as a condition of receiving care from us, or penalize patients for filing a complaint with HHS.