Notice of Privacy Practices

Martin Lan, MD PhD
19 West 34th Street, Penthouse Floor
New York, NY 10001
(212) 495-9627

Use and Disclosures of Health Information: Although under federal law we are permitted to use and disclose personal health information without consent or authorization for purposes of treatment, payment and health care operations, under New York state law and regulations, we will not release any personal health information to any third party except in the following circumstances:

A. With the patient's express consent for treatment and payment. This can be in writing, oral or implied. Examples: 1) A patient sends a written request to send a copy of his or her records to a physician who may be providing treatment to the patient. 2) A patient asks that we call the pharmacy to renew their medication 3) A patient asks that we submit a health insurance claim form to the patient's insurance carrier

B. Pursuant to the patient's written authorization, for other than treatment or payment purposes. Example: 1) We receive a request for medical information from a patient's potential employer

C. As otherwise permitted or required by federal or state law or regulation. Examples: 1) In an emergency situation 2) For child abuse or neglect reporting and investigation

D. For our internal operations. We will share information amongst collaborating and covering physicians, as well as office staff, to perform operations of the medical office. We will share with these business associates only the minimum amount of personal health information necessary for them to assist us.

Other Uses and Disclosures: In addition to uses and disclosures related to treatment, payment and health information without the patient's express consent or authorization for the following additional purposes:

Abuse, Neglect of 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 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 or 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 of, 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 the 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 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 persona 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 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 based on a good faith determination that such disclosure is necessary to prevent a serious and imminent threat to yourself, to identified individuals and to the public or in an emergency situation.

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.

Authorization: We will obtain an Authorization from the patient for all non-routine uses and disclosures of patient health information. An example of non-routine use or disclosure is the release of information in connection with a pre-employment medical evaluation. 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 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.

Minimum Necessary Rule: When using, disclosing or requesting protected health information, we will access only the minimum necessary amount of information. The 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: 1) In the course of treating a patient 2) Uses or disclosures made pursuant to a valid authorization 3) Uses or disclosures made to the individual 4) Disclosures to the Secretary of the Department of Health and Human Services 5) Uses or disclosures that are required by law 6) Uses or disclosures required to comply with the Privacy Rule

If we have employees, 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 a 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 1) the request is from a public official and the official represents that the request is for the minimum necessary information 2) the request is from another covered entity 3) 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 as overhearing a conversation, are not a violation of the Privacy Rule. We will not be health held liable for incidental disclosures otherwise authorized by the rule as long as we take reasonable efforts to safeguard and maintain the confidentiality of PHI.

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) All of the following identifiers of the individual (and relatives, employers or household names) are removed: a) names b) geographic subdivisions smaller than a State c) elements of dates (except year) directly related ot the individual and all ages for individuals over 89, unless aggregated into a single

category of age 90 or older d) telephone numbers, fax numbers, email addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate or 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 (eg. Indictment numbers or docket numbers). The entity must also 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.

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. 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 violations to HHS. A business associate agreement is not required in the case of disclosures by us to another health care provider for treatment purposes.

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

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 the 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 a) the minor consents to the health care service and no other consent is required by law b) 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 c) 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.

Patients' Rights: In order to exercise any of the patients' rights described below, the patient must submit a request in writing.

1) 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. 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*: a) If the request is not made in writing b) Request is for information compiled in connection with a legal proceeding c) Request is for information subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA) d) 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 e) The request is for information obtained in the course of research f) The 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.

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*: a) If access would reasonably be expected to cause substantial harm to the individual or others which would outweigh the need for such access b) If access is likely to endanger the life or physical safety of the individual or another person c) 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 of their right, if any, to request a review of the decision and how to do so.

2) Right to amend records: 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. If we are unable to satisfy th 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.

3) 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 solely out-of-pocket and such disclosure is not otherwise required by law

4) 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 alternative address, such as a P.O. box. We will accommodate reasonable requests for such confidential communications.

5) 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 disclosure, the name of the person or entity who received the information and their address if known, a brief description of the PHI disclosed and the reason for disclosure.

Customarily, a patient is not entitled to receive an accounting when the disclosure was made under the following circumstances: a) To the individual b) For routine (ie. treatment of payment) purposes c) For the internal operations of the medical office d) Incident to an otherwise permitted or required use or disclosure e) Pursuant to a valid authorization f) For notification purposes, such as to other individuals involved in the patient's health care g) For national security purposes h) To correctional institutions or law enforcement i) Made more than six year prior to the request

6) Right to request a copy of our Notice of Privacy Practices: A patient has a right to request a copy of our Notice of Privacy Practices or an electronic copy, if applicable.

Notice of Breach of Health Information: Breach means the acquisition, access, use or disclosure of PHI in violation of the HIPAA privacy rule that compromises the security or privacy of the information. The phrase "compromises the security or privacy of health information" means poses a significant risk of financial, reputational or other harm to the individual.

If a breach occurs and we determine that the breach poses significant harm to the individual, we will provide written notice to the individual affected as described below. In order to determine whether the breach poses significant harm to the individual, we will perform a fact-based risk assessment that includes consideration of the following factors 1) who or what type of entity received access to the information 2) steps taken to mitigate harm, such as obtaining satisfactory assurances (eg. A confidentiality agreement) from the recipient that the information will not be further used or disclosed, or will be destroyed 3) if the information was returned prior to it being accessed for an improper purpose and 4) the nature, type and amount of information used or disclosed

Notice to the individual: The required notice will be sent without unreasonable delay and in no case later than 60 calendar days of the discovery of the 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: 1) a brief description of what happened, the date of the breach, if known, and the date of discovery 2) the type of PHI involved in the breach 3) any precautionary steps the individual should take 4)

a description of what we are doing to investigate and mitigate the breach and prevent future breaches 5) contact information for us

The notice will be sent by first-class mail. If contact information for the individual in question is insufficient or out-of-date, we may contact the individual by telephone or other means, as appropriate, in addition to the written forms of notice.

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 cases later than 60 calendar days after discovery of the breach, notify prominent media outlets serving the State or jurisdiction.

Notice to the 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.

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.

Other Administrative Requirements: We will implement administrative, technical and physical safeguards to reasonably protect the privacy of PHI. We will safeguard PHI from intentional or unintentional disclosures in violation of the Privacy Rule and will limit incidental uses or disclosures of PHI.

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.

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 or Procedures.

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

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.

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

Complaints: If a patient believes his or her privacy rights have been violated, they may file a written complaint with us. The patient may also complain to the Secretary of Health and Human Services (HHS) by writing to Office for Civil Rights, US Department of Health and Human Services, 200 Independence Ave, SW Room 509F, Washington DC 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 the HHS as a condition of receiving care from us, or penalize patients for filing a complaint with HHS.