New HIPAA/HITECH Rules

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Health Information Technology for Economic and Clinical Health Act (HITECH)

To our patients: This notice describes how health information about you, as a patient of this practice, may be used and disclosed, and how you can get access to your health information. We are dedicated to maintaining the privacy of your health information and we are required by law to maintain the confidentiality of your health information. The final rule greatly enhances a patient's privacy protection, provides individuals new rights to their health information, and strengthens the government's ability to enforce the law.

In January of 2013, the HIPAA/HITECH Final Rule was issued. While the effective date of the Final Rule was March 26, 2013, the actual compliance date for most of the Rule's provisions is **September 23, 2013**. The Final Rule made significant changes to the HIPAA Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule. The rulemaking can be viewed in the Federal Register at https://www.federalregister.gov/public-inspection.

Overview of the New Rules

The changes that the Rules bring for most organizations include:

- The expansion of the definition of Business Associates to include subcontractors that access Protected Health Information;
- The imposition of direct liability under the Rules on Business Associates for compliance with certain HIPAA Privacy and Security Rule requirements;
- Additional and revised provisions that covered entities and Business Associates must include in their Business Associates Agreements, and a requirement for all existing Business Associates Agreements to comply with the new Rules by September 22, 2014;
- Additional disclosures in covered entities' HIPAA Privacy Notices, including informing individuals of their right to be notified of breaches of their Protected Health Information;
- Substantial lowering of the threshold for notification of affected individuals in the event of a breach of Private Health Information, and a requirement to conduct a documented risk assessment in the event notification is not provided in reliance on the harm threshold; and
- An expansion of individuals' rights to access their Protected Health Information.

Several other significant changes are primarily relevant to covered health care providers and certain non-covered third parties. These changes include:

- Individuals' enhanced ability to restrict disclosures of certain Protected Health Information; this revision affects mostly covered health care providers;
- Restrictions on the circumstances in which adherence programs can be conducted without individuals' authorization; these changes are most relevant to pharmacies and adherence communications providers and their service providers, and non-covered organizations that sponsor adherence communications; and
- Clarification of the circumstances in which providers of patient health record portals are subject to HIPAA; these requirements primarily concern covered and non-covered portal owners, sponsors and operators.

Business Associate Definition Scope Expansion

HIPAA and HITECH clarify the circumstances in which vendors are deemed to be Business Associates, and expand the definition of "Business Associate" to include most subcontractors that access Protected Health Information.

Vendors: HIPAA and HITECH clarify that vendors that require "routine" or "more than random" access to Protected Health Information are Business Associates, while those that act as "mere conduits" for or have "random access" to Protected Health Information continue to be outside the scope of the definition. This distinction is not based on whether a vendor or a subcontractor has an "opportunity" to access the data, but rather on whether that opportunity is "transient" or "persistent," with persistent opportunity more likely to deem a vendor a Business Associate. While entities that are "mere conduits" for Protected Health Information are not Business Associates, the HIPAA and HITECH emphasize that this exception is narrow. It is limited to entities providing data transmission services, including services that involve temporary storage of Protected Health Information that is incident to the transmission, i.e., courier services and their electronic equivalents, such as ISPs or telecoms.

Examples of vendors that are likely to be deemed Business Associates include:

- Providers of data transmission services, to the extent they require "routine access" to the Protected Health Information;
- Data storage or document storage vendors – whether or not they view the Protected Health Information they maintain;
- Operators of portals or other interfaces created on behalf of covered entities that allow patients to share their data with the covered entity; and
- Entities that provide oversight and governance for electronic heath information exchanges.

Subcontractors: HIPAA and HITECH also deem a Business Associate any subcontractor to the extent the subcontractor requires access to Protected Health Information (a "subcontractor" is an agent or other person other than a member of the workforce to whom a Business Associate delegates a covered function or activity). The "access" analysis applicable to first tier vendors applies equally to subcontractors. Importantly, a subcontractor that accesses Protected Health Information for the purposes of the Business Associate's *own* management or administration or legal compliance does not itself become a Business Associate by virtue of such access. While subcontractors whom the Rules deem Business Associates have direct obligations to comply with the Security Rule and certain provisions of the Privacy Rule, the new Rules continue to require Business Associates to obtain assurances of confidentiality of the Protected Health Information from non-Business Associate subcontractors.

Hybrid Entities: HIPAA and HITECH now require hybrid entities to include within the covered component of the entity Business Associate-like functions that were previously outside the covered component. An example of a hybrid entity includes an organization that is not generally in the business of providing health care, but, for example, operates on-site health clinics.

Direct Applicability of Certain Privacy and Security Requirements to Business Associates

Direct Applicability of Security Rule Requirements

HIPAA and HITECH make Business Associates directly responsible to regulators for complying with the Security Rule. The Department of Health and Human Services does not view this direct extension of liability as burdensome to Business Associates because, previously, covered entities were required to flow the requirements of the Security Rule to Business Associate via a contract.

Direct Applicability of Certain Privacy Rule Requirements

HIPAA and HITECH require Business Associates to:

- Use or disclose Protected Health Information only as permitted or required by required by law; any other use or disclosure of Protected Health Information would be a violation of the HIPAA Privacy Rule for which the Business Associate would be directly liable (such a violation would likely be deemed a breach subject to the requirement to notify affected individuals);

- Not use or disclose Protected Health Information in a manner that would violate the Privacy Rule if done by the covered entity;
- Disclose Protected Health Information when required by the Department of Health and Human Services to investigate or determine the Business Associate's compliance with HIPAA/HITECH;
- Disclose Protected Health Information to the covered entity, or to the individual or individual's designee to facilitate compliance with the individual's request for his or her electronic Protected Health Information;
- Provide an individual or the individual's designee with a copy of their Protected Health Information in an electronic format, if the individual so chooses, to the extent the entity maintains Protected Health Information in an electronic health record – *we do not use electronic records at this time and cannot send electronic records in any format.*
- Limit the Protected Health Information that Business Associates use, disclose or request to the minimum necessary to accomplish the intended purposes of the use, disclosure or request; and
- Respond to known noncompliance with the HIPAA/HITECH restrictions by their Business Associate subcontractors.

As a result, Business Associates are directly liable under HIPAA/HITECH for failures to fulfill these responsibilities, including:

- Uses and disclosures of Protected Health Information that are inconsistent with the Privacy Rule;
- Uses and disclosures of Protected Health Information that would violate the Privacy Rule if done by the covered entity;
- Failure to disclose Protected Health Information when required by the Secretary of the Department of Health and Human Services to investigate and determine the Business Associate's compliance with HIPAA/HITECH;
- Failure to disclose Protected Health Information to the covered entity, or to the individual to whom the information pertains, or the individual's designee, as necessary to fulfill covered entity's obligations to provide the information to the individual;
- Failure to make reasonable effort to limit Protected Health Information to the minimum necessary to accomplish the intended purposes of use or disclosure of, or request for, the Protected Health Information;
- Failure to enter into a Business Associates Agreement with subcontractors that access Protected Health Information on their behalf; and
- Failure to take reasonable action in response to a covered subcontractor's noncompliance with HIPAA/HITECH or the requirements of the Business Associates Agreement.

Business Associates' direct liability for violations of the Privacy Rule continues to be limited, and, except as articulated above, liability for Privacy Rule obligations that a covered entity may delegate to a Business Associate remains contractual to the covered entity.

Business Associate Agreement Updates

Key Date: While the Rules make significant changes to Business Associate Agreement requirements, covered entities and Business Associates (and Business Associates and their subcontractors) may continue to operate under existing agreements until *September 22, 2014*.

Requirements: The Rules now require Business Associates to enter into Business Associate Agreements with their subcontractors pursuant to the same requirements that apply to covered entities with respect to their first tier vendors. The Rules do not require covered entities to enter into Business Associate Agreements with their covered subcontractors.

Further, the Rules modify the provisions that govern the content of Business Associate Agreements, mandating that Business Associate Agreements:

- Require Business Associates that carry out covered entity's obligations under the Privacy Rule to comply with the requirements of the Privacy Rule that are applicable to that obligation;
- Require Business Associates to comply, where applicable, with the Security Rule in handling Protected Health Information;
- Require Business Associates to ensure that any subcontractors enter into a contract or other arrangements to protect the security of Protected Health Information; and

- Require Business Associates to report security incidents to covered entity "as required by Section 164.410 of the breach notification rules."

HIPAA Privacy Notice Updates

The Rules introduce several new requirements for content of HIPAA Privacy Notices and mandate the redistribution of the updated notices.

Additional Requirements for HIPAA Privacy Notices

In additional to the existing HIPAA Privacy Rule requirements, the new Rules require the HIPAA Privacy Notice to inform individuals that:

- They have a right to be notified following a breach of their unsecured Protected Health Information;
- They may be contacted to raise funds and have the right to opt out of receiving such communications;
- Most uses of and disclosures of Protected Health Information for marketing purposes and sales of Protected Health Information require the individual's authorization (entities that record or maintain psychotherapy notes also must state specifically that most uses or disclosures of such notes require the individual's authorization);
- Uses and disclosures not described in the Privacy Notice will be made only with the authorization from the individual; and
- Covered health care providers must state in their Privacy Notices that individuals have the right to restrict certain disclosures of Protected Health Information to a health plan when the individual (or any person other than the health plan) pays for treatment at issue out of pocket in full.

Redistribution of HIPAA Privacy Notices

The Rules deem the revisions to HIPAA Privacy Notices "material," and therefore, require redistribution of the updated HIPAA Privacy Notices. Accordingly, pursuant to the existing HIPAA Privacy Rule, covered entities must (1) prominently post the revised Privacy Notice (or a summary linked to the notice) on their site by the effective date of the changes (i.e., September 23, 2013 at the latest), and (2) provide the revised Privacy Notice in the covered entity's next annual mailing to affected individuals. If the notice is not provided via a website, the covered entity must provide it to affected individuals within 60 days of the effective date of the updated notice.

Breach Notification Requirement Update

The Rules introduce comprehensive updates to the requirements governing the investigation and response to potential breaches of electronic Protected Health Information. Specifically, the Rules *lower the threshold for notification* of affected individuals in the event of unauthorized access to Protected Health Information by:

- Abandoning the current harm threshold that required notification *only if* the individuals affected by a breach were exposed to a "significant risk of financial, reputation or other harm;" and instead
- Presuming that notification is required in all circumstances, except when: The covered entity conducts a risk assessment that establishes that there is a "low probability" of compromise of the Protected Health Information; or One of the existing exceptions to the definition of the breach applies (i.e., unintentional good faith acquisition, access, or use of Protected Health Information by a workforce member; inadvertent disclosure between two individuals who are otherwise authorized to access the Protected Health Information; or disclosure to an unauthorized person who would not reasonably have been able to retain such information).

The required risk assessment to determine the probability of Protected Health Information compromise must be thorough, completed in good faith, and reach conclusions that are reasonable. To meet these requirements, the risk assessment must consider at least:

- The nature and extent of the Protected Health Information involved (i.e., types of identifiers, likelihood of re-identification, and the amount of data and its sensitivity);
- The type of unauthorized person who used the Protected Health Information or to whom the data was disclosed;
- Whether the Protected Health Information was actually acquired or viewed; and
- The extent to which risk to the Protected Health Information has been mitigated.

The Rules provide detailed guidance on considering and weighing these factors. The Department of Health and Human Services indicated that it will issue further guidance on conducting risk assessments of frequently-occurring scenarios.

Revised Restriction on Sale of Protected Health Information

The Rules define the sale of Protected Health Information as any disclosure of the information for which the covered entity or Business Associate receives remuneration from or on behalf of the recipient. Such remuneration may be direct or indirect, and financial or non-financial. The Rules prohibit such sales, except with a written authorization of the individual to whom the Protected Health Information pertains. The authorization must explain (in terms left to the disclosing entity's discretion) that the disclosure will result in the covered entity or Business Associate receiving remuneration for the Protected Health Information.

The Rules permit disclosures of Protected Health Information without the individual's authorization pursuant to several exceptions, such as:

- Disclosures by a Business Associate in connection with performance of services for a covered entity (or by a subcontractor for a first tier Business Associate vendor);
- Disclosures to individuals to whom the Protected Health Information pertains to comply with the individual's request for access to the Protected Health Information or accounting for the disclosure of the information;
- Disclosures of Protected Health Information required by law;
- Disclosures associated with grants or other arrangements to perform studies; and
- Certain disclosures for public health purposes and for research purposes (if the remuneration reflects a reasonable fee to cover the cost of data preparation and disclosures).

Entities that disclose Protected Health Information, should verify that the disclosures do not constitute a "sale" under the new Rules. The revised requirements will apply to any disclosures after September 25, 2013.

Fundraising Restrictions

The Rules require fundraising communication to include a method for the recipient to opt out from receiving such communications. The opt-out methods may not burden recipients with more than nominal cost, and may include a toll-free number or an email address, but *not* a requirement to write and send a letter, for example, which would be considered too burdensome.

The Rules also clarify that the Protected Health Information that may be used for fundraising purposes is limited to individuals' names, addresses, other contact information, age, gender, date of birth, dates during which the individual received the relevant health care, general department of treatment, and treatment outcome information.

The Rules prohibit conditioning of treatment or payment on the individual's choice with respect to receiving fundraising communications.

Marketing / Changes in Adherence Communications Requirements

The new Rules require authorization for all treatment and health care operations communications where the covered entity or the covered entity's Business Associate receives financial remuneration *specifically* for making the communication from a third party whose product or service is being marketed. The Rules, however, exempt from this authorization requirement refill reminders or communications about a drug or biologic agent currently being prescribed to the individual. The Department of Health and Human Services clarified that "adherence communications encouraging individuals to take their prescribed medications as directed fall within the scope of the exception." However, for this exception to apply, the financial remuneration for sending the communication must be "reasonably related" to the cost of making the communication, i.e., limited to the costs of drafting, printing and mailing the communications, and associated costs. If, however, the remuneration includes an additional payment (e.g., to encourage covered entity's or its Business Associate's continued willingness to send the communications), the exception likely will not apply, and the patient's authorization will be required to send the communications.

Expansion of Individuals' Rights

HIPAA and HITECH expand individuals' rights to restrict certain disclosures of their Protected Health Information and enhance individuals' access to their Protected Health Information.

Protected Health Information *Disclosure Restrictions – Applicable Primarily to Covered Health Care Providers*

HIPAA and HITECH specifically require covered entities to comply with individuals' requests to restrict the disclosure of their information; to the extent the disclosure satisfies three conditions:

- The disclosure is for purposes of carrying out payment or healthcare operations;
- The disclosure is not otherwise required by law or regulations (including Medicare, Medicaid, and other requirements); and
- The Protected Health Information subject to the request pertains solely to a health care item or service for which the individual (or family member, or anyone other than the health plan) paid in full.

The requirement to restrict disclosure would also bar disclosures to Business Associates. Under HIPAA and HITECH, the individual retains the discretion to determine for which services he or she wants to pay out of pocket.

A disclosure of Protected Health Information in violation of this requirement would violate the Privacy Rule and, therefore, potentially trigger breach response and notice obligations.

Enhanced Protected Health Information *Access Rights*

HIPAA and HITECH require covered entities to provide an individual or the individual's designee with access to the individual's Protected Health Information, if an individual requests an electronic copy of his or her Protected Health Information that a covered entity maintains in the ordinary course of business. (*Currently, we do not use any electronic medical records.)*

Covered entities must produce the information in the form and format requested by the individual to the extent it is readily producible in such form and format. Otherwise the Protected Health Information must be provided to the individual in another agreed-upon computerized format, such as MS Word or Excel, text, HTML or PDF. A covered entity that uses or maintains electronic health records with respect to the requested information must provide a copy of the information in an electronic format. (*Currently, we do not use any electronic medical records.)*

The rule establishes a 30-day period (with an extension available under certain circumstance) for covered entities to comply with an access request, and allows covered entities to charge certain reasonable fees to produce the information.

One of the key goals of the enhanced access rights is to allow individuals better access to electronic health records and to facilitate individuals' ability to direct the transmission of their records to, for example, an online portal on which the individual maintains personal health records.

To read the entire Final Rule - *http://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/index.html*

Click on: Read the Final Rule in the Federal Register

If you need help filing a complaint or have a question about the complaint package, please e-mail OCR at OCRMail@hhs.gov.

Patient Bill of Rights and Responsibility (HIPAA 1996)

We believe that patients want to understand and participate in their health care. We also believe that patients can better participate if they know their rights and responsibilities. The following information summarizes these rights and responsibilities for our patients. When the patient is a minor, these rights also apply to the parents or guardians.

Access to Care
You have the right to impartial access to treatment or accommodations that are available or medically indicated, regardless of your race, creed, sex, national origin, disability or sources of payment for care.

Consent
You have the right to reasonable, informed participation in decisions involving your health care. You will be asked by your physician to sign consent for medical and surgical procedures. You have the right to prepare a Directive to Physician, Family and Surrogates (Living Will) or a Medical Power of Attorney for Health Care. With an advance directive, you can direct your physician to provide or to limit life-sustaining treatment, if you develop a terminal medical condition. You will not be discriminated against based on whether or not you complete an advance directive.

Consideration
All patients are responsible for following rules and regulations and for being considerate of the rights of others.

Consultation
You have the right to consult with a specialist at your own request and expense.

Financial Responsibilities
You are responsible for ensuring that the financial obligations of your health care are fulfilled. We will bill your insurance company for its portion if you provide insurance billing information. Any unpaid balance by your insurance company will be your responsibility.

Regardless of the source of payment for your care, you have the right to request and receive an itemized and detailed explanation of your total bill for services rendered.

Following Instructions
You are responsible for following the treatment plan recommended by your doctors, nurses and other caregivers, and for reporting side effects of any treatments to your doctor. If you refuse treatment or fail to follow the directions of your physicians, your care may be affected.

Giving & Receiving Information
You are responsible for providing accurate and complete information about your health and for reporting changes in

your condition. In addition, you have the right to obtain, from the health care professional responsible for your care, complete and current information about your diagnosis (to the degree known), treatment and any known prognosis.

Identity
You have the right to know the identity and professional status of individuals providing service to you and to know which physician or other practitioner is primarily responsible for your care.

Privacy & Confidentiality
The Health Insurance Portability and Accountability Act of 1996, also known as HIPAA, mandates regulations that govern privacy, security and electronic transaction standards. The primary purpose of this federal law is to provide standards to facilitate the electronic exchange of health information, provide individuals with better access to their health information and standardize this access among states, decrease health care fraud and abuse, and most importantly to protect your personal health information.

Our office has special concern for confidentiality in the workplace. Safeguarding patients' health information is not only a legal requirement but also an important ethical obligation. As a health care provider, staff members are entrusted with clinical information regarding our patients. We recognize that medical and billing records are highly confidential and must be treated with great respect and care by all staff with access to this information. Our policy regarding confidentiality of protected health care information reflects our strong commitment to protecting the confidentiality of our patients' medical records and clinical information. The "Noticy of Privacy Practices" handout given to every patient, explains our policies in more detail.

Under HIPAA guidelines, we will provide you with an opportunity to restrict or prohibit some or all disclosures unless emergency circumstances prevent you from objecting.

Refusal of Treatment
You may refuse treatment to the extent permitted by law.

Release of Information
After receiving treatment, you may require copies of your medical records.

Respect & Dignity
You have the right to considerate, respectful care at all times and under all circumstances.

HIPAA (4-14-2003)

Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This is your Health Information Privacy Notice from **TOM SLOAN, M.D.** (referred to as We or Us). This notice is effective April 14, 2003.

This notice provides you with information about the way in which We protect Personal Health Information ("PHI") that We have about you. PHI includes individually identifiable information which relates to your past, present or future health, treatment or payment for health care services. This notice also explains your rights with respect to PHI.

The Health Insurance Portability and Accountability Act ("HIPAA") requires Us to: Keep PHI about you private; provide you this notice of our legal duties and privacy notices with respect to your PHI; and follow the terms of the notice that are currently in effect.

Use and Disclosure of PHI

We obtain PHI in the course of providing and/or administering health insurance benefits for you. In administering your benefits, We may use and/or disclose PHI about you and your dependents. The following are some examples, however, not every use or disclosure in a category will be listed:

- **For Health Care Payment Purposes:** For example, We may use and disclose PHI to administer and process payment of benefits under your insurance coverage, determine eligibility for coverage, claims or billing information, conduct utilization reviews, or to another entity or health care provider for its payment purposes.

- **For Health Care Operations Purposes:** For example, We may use and disclose PHI for underwriting and rating of the plan, audits of your claims, quality of care reviews, investigation of fraud, care coordination, investigate and respond to complaints or appeals, provider treatment review and provision of services.

- **For Treatment Purposes.** For example, We may use and disclose PHI to health care providers to assist in their treatment of you. We do not provide health care treatment to you directly.

- **For Health Services.** For example, We may use your medical information to contact you to give you information about treatment alternatives or other health related benefits and services that may be of interest to you as part of large case management or other insurance related services.

- **For Data Aggregation Purposes.** For example, We may combine PHI about many insureds to make plan benefit decisions, and the appropriate premium rate to charge.
- **To You About Dependents.** For example, We may use and disclose PHI about your dependents for any purpose identified herein. We may provide an explanation of benefits for you or any of your dependents to you.

- **To Business Associates.** For example, We may disclose PHI to administrators who are contracted with Us who may use the PHI to administer health insurance benefits on our behalf and such administrators may further disclose PHI to their contractors or vendors as necessary for the administration of health insurance benefits.

If your state has adopted a more stringent standard regarding any of the above uses or disclosures of your PHI, those standards will be applied.

Additional Uses or Disclosures. We may also disclose PHI about you for the following purposes:

- To comply with legal proceedings, such as a court or administrative order, subpoena or discovery requests.
- To law enforcement officials for limited law enforcement purposes.
- To a family member, friend or other person, for the purpose of helping you with your health care or with payment for your health care, if you are in a situation such as a medical emergency and you cannot give your agreement to the Plan to do this.
- To your personal representatives appointed by you or designated by applicable law.
- For research purposes in limited circumstances.
- To a coroner, medical examiner, or funeral director about a deceased person.
- To an organ procurement organization in limited circumstances.
- To avert a serious threat to your health or safety or the health or safety of others.
- To a governmental agency authorized to oversee the health care system or government programs.
- To the Department of Health and Human Services for the investigation of compliance with HIPAA or to fulfill another lawful request.
- To federal officials for lawful intelligence, counterintelligence, national security purposes and to protect the president.
- To public health authorities for public health purposes.
- To appropriate military authorities, if you are a member of the armed forces.
- In accordance with a valid authorization signed by you.

Your Rights Regarding PHI That We Maintain About You

You have various rights as a consumer under HIPAA concerning your PHI. You may exercise any of these rights by writing to Us in care of **Allen J. Flood, 2 Madison Avenue, Larchmont, NY, 10538, Attention: HIPAA Privacy Office:**

- You have the right to inspect and copy your PHI. If you request a copy of the information, We may charge a fee for the costs of copying, mailing or other supplies associated with your request.
- You have the right to ask Us to amend the PHI that is contained in a "designated record set", e.g., information used to make enrollment, eligibility, payment, claims adjudication and other decisions. You have the right to request an amendment for as long as we maintain the PHI. Requests must be made in writing and include the reason for the request. We may deny the request if the PHI is accurate and complete or if we did not create the PHI.
- You have the right to request a list of our disclosures of the PHI. Your request must state a time period, may not include dates before April 14, 2003 and may not exceed a period of six years prior to the date of your request. If you request more than one list in a year, We may charge you the cost of providing the list. We will notify you of the cost and you may withdraw or modify your request before any costs are incurred. Any list of disclosures provided by Us will not include disclosures made for payment, treatment or healthcare operations; made to you or persons involved in your care; incidental disclosures, authorized disclosures, for national security or intelligence purposes or to correctional institutions.
- You have the right to request to restrict the way We use or disclose PHI regarding treatment, payment or health care operations. You also have the right to request to restrict the PHI We disclose about you to someone who is involved in your care or the payment for your care. We are not required to agree to your request. If We do agree, We will comply with your request unless the information is needed to provide you emergency treatment. Your request must be in writing and state (1) what information you want to restrict; (2) whether you want to restrict our use, disclosure or both; and (3) to whom you want the restrictions to apply.
- Uses and disclosures of your PHI, other than those listed above, require prior written authorization from you. You may revoke that authorization at any time by writing to Us at the address at the end of this notice.
- You have the right to request that We communicate personal information to you in a certain way or at a certain location. Your request must specify how or where you wish to be contacted. We will comply with reasonable requests.
- You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time. Even if you have agreed to receive this notice electronically, you are still entitled to a paper copy of this notice upon request. You may request a paper copy of this notice by calling Us at 1-800-951-6206, select HIPAA or submitting the request to the Combined Life Insurance Company of New York, 5050 Broadway, Chicago, IL 60640 Attn: HIPAA Privacy Office.

Complaints

If you believe your privacy rights have been violated, you may file a complaint with Us. When filing a complaint, include your name, address and telephone number and We will respond. All complaints must be submitted in writing to Combined Life Insurance Company of New York, 5050 Broadway, Chicago, IL 60640 Attn: HIPAA Privacy Office. You may also contact the Secretary of the Department of Health and Human Services. You will not be retaliated against for filing a complaint.

Changes To This Notice

We reserve the right to modify this Privacy Notice and our privacy policies at any time. If We make any modifications, the new terms and policies will apply to all PHI before and after the effective date of the modifications that We maintain. If We make material changes, We will update you at the next visit.

All questions and requests regarding your rights under this Notice should be sent to:

Tom Sloan, M.D.
1120 Medical Plaza Drive, Suite 100 The Woodlands, TX 77380
Phone: 281-363-2266 Fax: 281-363-2279

Website: tomsloanmd.com

Acknowledgement of HIPPA/HITECH updates
and
Notice of Privacy Practices

I acknowledge that I have been notified there is a new notice and updates to HIPAA/HITECH/Notice of Privacy Practices that can be viewed online at www.tomsloanmd.com and the notice has been made available to me in the office as well.

_____ _____
Patient Name (Please print) Date

_____
Signature