

Notice of Privacy Policies

This notice describes how your medical information may be used and/or disclosed and how you can get access to this information. Please review this document. Your privacy is of the utmost importance to us. The following is our privacy promise to you, our patient.

We are committed to preserving, disclosing, and using your protected health information responsibly. Your privacy is a top priority at our practice. This Notice applies to all protected health information (PHI) as defined by federal regulations.

Understanding Your Health Record/Information

Each time you visit Mara Thornberg, a record of your visit is made. Typically, this record contains your symptoms, examination and test results, diagnoses, treatment, and a plan for future care or treatment. This information, often referred to as your health or medical record, serves as a:

- Basis for planning your care and treatment
- Means of communication among the many health professionals who contribute to your care
- Legal document describing the care you received
- Means by which you or a third-party payer can verify that services billed were actually provided
- A source of data for medical research
- A source of information for public health officials charged with improving the health of the state and the nation
- A source of data for our planning and marketing
- A tool with which we can assess and continually work to improve the care we render and the outcomes we achieve

We wish to help you better understand what is in your record and how your health information will be used and disclosed. By being open with you, we feel this will ensure accuracy, better understanding who, what, when, where, and why others may access your health information, and make more informed decisions when authorizing disclosure to other parties.

Your Health Information Rights

Please realize that your health record is the physical property of Mara Thornberg, LPC; however, the information belongs to you. You have the following rights regarding your protected health information (PHI):

- Obtain a paper copy of this notice of informational practices upon request
- Inspect and copy your health records as provided for in 45 CFR 164.524
- Amend your health record as provided in 45 CFR 164.524
- Obtain an accounting of disclosures of your health information as provided in 45 CFR 164.524
 - Request communications of your health information by alternative means or at alternative locations
- Request a restriction on certain uses and disclosures of your information as provided by 45 CFR 164.524

- Revoke your authorization to use or disclose health information except to the extent that action has been already been take

Our Responsibilities

- Maintain the privacy of your health information
- Provide you with this notice as to our legal duties and privacy practices with respect to information we collect and maintain about you
- Abide by the terms of this notice
- Notify you if we are unable to agree to a requested restriction
- Accommodate reasonable requests you may have to communicate health information by alternative means or at alternative locations.

We reserve the right to change our practices if we feel it is necessary to protect your information. The new provisions effective for all protected health information (PHI) we maintain will be mailed to you if necessary. Should our information practices change, we will mail a revised notice to the address you have supplied to us. We will not use or disclose your health information without your authorization, except as described in this notice. We will also discontinue to use or disclose your health information after we have received a written revocation of the authorization according to the procedures included in the authorization. This will not affect disclosures made in good faith of the original authorization.

For More Information or to Report a Problem

If you have questions, and would like additional information, you may contact the practice's Privacy Officer. If you believe your privacy rights have been violated, you can file a complaint with the practice's Privacy Officer or with the Office for Civil Rights, U.S. Department of Health and Human Services. We will not take any retaliation for filing a complaint with either the Privacy Officer or the Office for Civil Rights.

Office for Civil Rights

U.S. Department of Health and Human Services
200 Independence Avenue, SW
Room 509F, HHH Building
Washington, DC 20201

Examples of Disclosures for Treatment, Payment and Health Operations

We will use your health information for treatment: Information obtained by a nurse, physician, or other member of your health care team will be recorded in your record and used to determine the course of treatment that should work best for you. Your provider will document in your record his or her expectations of the members of your health care team. Members of your health care team will then record the actions they took and their observations. In that way, the provider will know how you are responding to treatment. We will also provide your provider or a subsequent health care provider with copies of various reports that should assist him or her in treating you if you are referred to a specialist or other healthcare provider or in a situation where you are released from treatment.

We will use your health information for payment: A bill may be sent to you or a third-party payer. The information on or accompanying the bill may include information that identifies you, as well as your diagnoses, procedures, and supplies used.

We will use your health information for regular health operations: Members of the medical staff may use information in your health record to assess the care and outcomes in your case and others like it. This information will then be used in an effort to continually improve the quality and effectiveness of the healthcare and service we provide. We may also use your mailing and contact information to send you notices from time to time to get such important notices to you.

Calls and Messages: We may contact you by phone to confirm your appointment. Messages may be left on answering machines to this effect. In the case of a missed appointment, we may call to make sure everyone is all right and to reschedule the appointment for a later date.

Business Associates: There are some services provided in our organization through contacts with business associates. Examples include emergency departments, medical laboratories, etc. When these services are contracted, we may disclose your health information to our business associate so that they can perform the job we have asked them to do and bill you or your thirdparty payer for services rendered. To protect your health information, however, we require the business associate to appropriately safeguard your information.

Notification: We may, with your permission, use or disclose information to notify or assist in notifying a family member, personal representative, or another person responsible for your care, your location, and general condition.

Communication with family: Health professionals, using their best judgment, may disclose to a family member, other relative, close personal friend, or any other person you identify, health information relevant to that person's involvement in your care or payment related to your care.

Research: We may disclose information to researchers when their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your health information.

Marketing: We may contact you to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to you.

Food and Drug Administration (FDA): We may disclose to the FDA health information relative to adverse events with respect to food, supplements, product and product defects, or post marketing surveillance information to enable product recalls, repairs, or replacements.

Workers Compensation: We may disclose health information to the extent authorized by and to the extent necessary to comply with laws relating to workers compensation or other similar programs established by law.

Public Health: As required by law, we may disclose your health information to public health or legal authorities charged with preventing or controlling disease, injury, or disability. **Law**

Enforcement: We may disclose health information for law enforcement purposes as required by law or in response to a valid subpoena. Federal law makes provision for your health information to be released to an appropriate health oversight agency, public health authority or attorney, provided that a work force member or business associate(s) believes in good faith that

we have engaged in unlawful conduct or have otherwise violated professional or clinical standards and are potentially endangering one or more patients, workers, or the public.

HIPAA Overview

HIPAA Privacy and Security Regulations:

A Synopsis of the Relevant Mandates of Title II (Administrative Simplification)
Health Insurance Portability and Accountability Act of 1996
Public Law 104-191

In 1996, President Clinton signed the Health Insurance Portability and Accountability Act (HIPAA). This law mandates action that seeks to: 1) ensure continuity of healthcare coverage for individuals changing jobs; 2) impact on the management of health information; 3) simplify the administration of health insurance; and 4) combat waste, fraud, and abuse in health insurance and health care.

Title II: The Security and Privacy Mandates

Title II of the HIPAA law (also known as Administrative Simplification) includes requirements for ensuring the security and privacy of individuals' medical information. The standards aim to maintain the right of individuals to keep private information about themselves. The Department of Health and Human Services is charged with developing the issuing regulations to address these requirements. The final privacy rule was released April 14, 2001; compliance is now required by April 2003. The security rule is being finalized; the released date is expected to be June/July 2001.

Protected Information

HIPAA regulations protect medical records and other "individually identifiable health information" (communicated electronically, on paper, or orally) that are created or received by covered health care entities that transmit information electronically.

"Individually identifiable health information..." includes

- any information, including demographic information collected from an individual; and
- any information that identifies an individual, or could be reasonably believed to identify an individual

HIPAA protects "individually identifiable health information" which...

- relates to the past, present, or future physical or mental health condition of an individual, the provision of health care or the payment for such care
- is maintained or transmitted, and is (or has been) in electronic form
- is used or disclosed by covered entities

What is the difference between Security and Privacy?

Security – relates to the means (process and technology) by which an entity protects the privacy of health information. The goals of security measures are to keep information secured, and decrease the means of tampering, destruction, or inappropriate access. There are four categories of requirements:

- Administrative Procedures – documented, formal practices to protect data
- Physical Safeguards – protect data from fire, other natural and environmental hazards, and intrusion

- Technical Security Services – protect information and control individual access to information
 - Technical Security Mechanisms – guard against unauthorized access to data over communications network

Privacy – refers to the individual’s right to keep certain information private, unless that information will be used or disclosed with his or her permission. Privacy topics include:

- Scope of Providers who must Comply
- Rights of Individuals
- Consent/Authorization Issues/Procedures/Processes
- Business Associates Requirements
- Organized Health Care Arrangements

Note: there are civil penalties when entities/individuals violate the privacy rule. Security and privacy are very intertwined – security assures privacy.