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 practice uses and discloses health information about you for treatment, to obtain payment for treatment, for administrative purposes, and to evaluate the quality of care that you receive. This notice describes our privacy practices. You can request a copy of this notice at any time. For more information about this notice or our privacy practices and policies, please contact us at the address listed on page 4 of this Notice.

Treatment, Payment, and Health Care Operations Treatment
We are permitted to use and disclose your medical information to persons involved in your treatment. For example, your care may require the involvement of a specialist. When we refer you to a specialist, we will share some or all of your medical information with that medical provider to facilitate the delivery of care.
OR
When we provide treatment, we may request that your primary care physician share your medical information with us. Also, we may provide your primary care physician information about your particular condition so that he or she can appropriately treat you for other medical conditions, if any.

Payment
We are permitted to use and disclose your medical information to bill and collect payment for the services provided to you. For example, we may complete a claim form to obtain payment from your insurer or HMO. The form will contain medical information that your insurer or HMO needs to approve payment to us, such as a description of the medical service provided to you.

Health Care Operations
We are permitted to use or disclose your medical information for the purposes of health care operations, which are activities that support this practice and ensure that quality care is delivered. For example, we may engage the services of a professional to aid this practice in its compliance programs. That person will review billing and medical files to ensure we maintain our compliance with regulations and the law.
OR
We may ask another physician to review this practice's charts and medical records to evaluate our performance so that we may ensure that only the best health care is provided by this practice.

Disclosures That Can Be Made Without Your Authorization
There are situations in which we are permitted by law to disclose or use your medical information without your written authorization or an opportunity to object. In other situations, we will ask for your written authorization before using or disclosing any identifiable health information about you. If you choose to sign an authorization to disclose information, you can later revoke that authorization, in writing, to stop future uses and disclosures. However, any revocation will not apply to disclosures or uses already made or taken in reliance on that authorization.

Public Health, Abuse or Neglect, and Health Oversight
We may disclose your medical information for public health activities. Public health activities are mandated by federal, state, or local government for the collection of information about disease, vital statistics (like births and death), or injury by a public health authority. We may disclose medical information, if authorized by law, to a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition. We may disclose your medical information to report reactions to medications, problems with products, or to notify people of recalls of products they may be using. We may also disclose medical information to a public

agency authorized to receive reports of child abuse or neglect. Texas law requires physicians to report child abuse or neglect. Regulations also permit the disclosure of information to report abuse or neglect of elders or the disabled. We may disclose your medical information to a health oversight agency for those activities authorized by law. Examples of these activities are audits, investigations, licensure applications and inspections which are all government activities undertaken to monitor the health care delivery system and compliance with other laws, such as civil rights laws.

Legal Proceedings and Law Enforcement
We may disclose your medical information in the course of judicial or administrative proceedings in response to an order of the court (or the administrative decision-maker) or other appropriate legal process. Certain requirements must be met before the information is disclosed. If asked by a law enforcement official, we may disclose your medical information under limited circumstances provided that the information:

- Is released pursuant to legal process, such as a warrant or subpoena;
- Pertains to a victim of crime and you are incapacitated;
- Pertains to a person who has died under circumstances that may be related to criminal conduct;
- Is about a victim of crime and we are unable to obtain the person's agreement;
- Is released because of a crime that has occurred on these premises; or
- Is released to locate a fugitive, missing person, or suspect.

We may also release information if we believe the disclosure is necessary to prevent or lessen an imminent threat to the health or safety of a person.

Workers' Compensation
We may disclose your medical information as required by the Texas workers' compensation law.

Inmates
If you are an inmate or under the custody of law enforcement, we may release your medical information to the correctional institution or law enforcement official. This release is permitted to allow the institution to provide you with medical care, to protect your health or the health and safety of others, or for the safety and security of the institution.

Military, National Security and Intelligence Activities, Protection of the President
We may disclose your medical information for specialized governmental functions such as separation or discharge from military service, requests as necessary by appropriate military command officers (if you are in the military), authorized national security and intelligence activities, as well as authorized activities for the provision of protective services for the President of the United States, other authorized government officials, or foreign heads of state.

Research, Organ Donation, Coroners, Medical Examiners, and Funeral Directors
When a research project and its privacy protections have been approved by an Institutional Review Board or privacy board, we may release medical information to researchers for research purposes. We may release medical information to organ procurement organizations for the purpose of facilitating organ, eye, or tissue donation if you are a donor. Also, we may release your medical information to a coroner or medical examiner to identify a deceased or a cause of death. Further, we may release your medical information to a funeral director where such a disclosure is necessary for the director to carry out his duties.

Required by Law
We may release your medical information where the disclosure is required by law.

Your Rights Under Federal Privacy Regulations
The United States Department of Health and Human Services created regulations intended to protect patient privacy as required by the Health Insurance Portability and Accountability Act (HIPAA). Those regulations create

several privileges that patients may exercise. We will not retaliate against a patient that exercises their HIPAA rights.

Requested Restrictions
You may request that we restrict or limit how your protected health information is used or disclosed for treatment, payment, or healthcare operations. We do NOT have to agree to this restriction, but if we do agree, we will comply with your request except under emergency circumstances.

To request a restriction, submit the following in writing: (a) The information to be restricted, (b) what kind of restriction you are requesting (i.e. on the use of information, disclosure of information or both), and (c) to whom the limits apply. Please send the request to the address and person listed below. You may also request that we limit disclosure to family members, other relatives, or close personal friends that may or may not be involved in your care.

Receiving Confidential Communications by Alternative Means
You may request that we send communications of protected health information by alternative means or to an alternative location. This request must be made in writing to the person listed below. We are required to accommodate only *reasonable* requests. Please specify in your correspondence exactly how you want us to communicate with you and, if you are directing us to send it to a particular place, the contact/address information.

Inspection and Copies of Protected Health Information
You may inspect and/or copy health information that is within the designated record set, which is information that is used to make decisions about your care. Texas law requires that requests for copies be made in writing and we ask that requests for inspection of your health information also be made in writing. Please send your request to the person listed below.
We can refuse to provide some of the information you ask to inspect or ask to be copied if the information:

- Includes psychotherapy notes.
- Includes the identity of a person who provided information if it was obtained under a promise of confidentiality.
- Is subject to the Clinical Laboratory Improvements Amendments of 1988.
- Has been compiled in anticipation of litigation.

We can refuse to provide access to or copies of some information for other reasons, provided that we provide a review of our decision on your request. Another licensed health care provider who was not involved in the prior decision to deny access will make any such review. Texas law requires that we are ready to provide copies or a narrative within 15 business days of your request. We will inform you of when the records are ready or if we believe access should be limited. If we deny access, we will inform you in writing. HIPAA permits us to charge a reasonable cost based fee. The Texas State Board of Medical Examiners (TSBME) has set limits on fees for copies of medical records that under some circumstances may be lower than the charges permitted by HIPAA. In any event, the *lower* of the fee permitted by HIPAA or the fee permitted by the TSBME will be charged.

Amendment of Medical Information
You may request an amendment of your medical information in the designated record set. Any such request must be made in writing to the person listed below. We will respond within 60 days of your request. We may refuse to allow an amendment if the information:

- Wasn't created by this practice or the physicians here in this practice.
- Is not part of the Designated Record Set.
- Is not available for inspection because of an appropriate denial.
- If the information is accurate and complete.

Even if we refuse to allow an amendment you are permitted to include a patient statement about the information at issue in your medical record. If we refuse to allow an amendment we will inform you in writing. If we approve the amendment, we will inform you in writing, allow the amendment to be made and tell others that we know have the incorrect information.

Accounting of Certain Disclosures
The HIPAA privacy regulations permit you to request, and us to provide, an accounting of disclosures that are other than for treatment, payment, health care operations, or made via an authorization signed by you or your representative. Please submit any request for an accounting to the person listed below. Your first accounting of disclosures (within a 12 month period) will be free. For additional requests within that period we are permitted to charge for the cost of providing the list. If there is a charge we will notify you and you may choose to withdraw or modify your request *before* any costs are incurred.

Right to Receive Notice of a Breach
We are required to notify patients by First Class Mail or by email (if the individual has indicated a preference to receive information by email), of any breaches of UNSECURED Protected Health Information as soon as possible following the discovery of the breach. Our Organization will investigate any 'event' or incident' where a patient's PHI is known or thought to have been wrongfully disclosed. If it is determined that a breach has occurred both the patient, the Federal and State government will be notified according to state regulations. It is important to remember that PHI in Systems that are encrypted are not subject to breach (they are considered to be in the 'breach safe harbor'); however HIPAA violations can still occur, therefore all 'events or incidents must be investigated and corrective actions taken, even if a wrongful disclosure is not determined to be a breach.

All of the above documentation must be kept for the minimum 6-year HIPAA retention period.

Security
This section of this guide is intended to give a general overview of the security compliance measures undertaken by this Organization. This summary is not intended to be an exhaustive list, rather an overview of the more common safeguards we employ. Please refer to our detailed polices, any written procedures and Risk Assessments for more information and statutory language or specific rules.

Risk Assessment – Risk Assessment to be updated routinely as the Organization's safeguards materially change, but not less than yearly.

Workforce Termination –Workforce members who are terminated will have their access to computer systems and networks removed immediately.

Access to PHI – All appropriate access to PHI is secured through the use of passwords which are changed routinely; of appropriate strength and unique to each user. All access to PHI is through formal logon. Remote access is via secured data in transit and no data is stored on mobile devices.

Password Management –Passwords expire and must be changed every 90 days. Use of more secure passwords, i.e. multiple digit letter number combinations is required.

Auto Log-off –Users are logged off of PCs and Servers after periods of inactivity.

Back-up and Restoration –Multiple levels of routine and remote back-ups are maintained. They are tested for restoration integrity and are encrypted data at rest and in transit.

Malware Prevention – Anti-virus, firewall(s), intrusion monitoring, detection and prevention and similar safeguards are all up to date and continually maintained.

Physical Security – The Organization has locks, alarms and segregated records and computers / monitors for patient areas, as practical. Maintenance records for all physical security items are kept for the 6-year HIPAA documentation retention period.

Media and Devices –mobile devices are only used by only via secure connection and never store PHI.

Audit Controls – Athena maintains an audit log of all user activities which is monitored at least quarterly for inappropriate access, use or disclosure. We also monitor error and technical logs for inappropriate activity on a routine basis.

Security and Privacy Training - Workforce members are trained at new hire, at least annually thereafter and whenever there are material changes to the privacy / security rules or job roles which require a different level of training. Security and privacy reminders are discussed at staff meetings and other opportunities. Tests and documentation of the training is kept for the 6-year HIPAA documentation retention period.

Appointment Reminders, Treatment Alternatives, and Other Health-Related Benefits
We may contact you by telephone, mail, and/or email to provide appointment reminders, information about treatment alternatives, or other health-related benefits and services that may be of interest to you.

Complaints
If you are concerned that your privacy rights have been violated, you may contact the person listed below. You may also send a written complaint to the United States Department of Health and Human Services. We will not retaliate against you for filing a complaint with the government or us. The contact information for the United States Department of Health and Human Services is:
U.S. Department of Health and Human Services
HIPAA Complaint
7500 Security Blvd., C5-24-04
Baltimore, MD 21244

Our Promise to You
We are required by law and regulation to protect the privacy of your medical information, to provide you with this notice of our privacy practices with respect to protected health information, and to abide by the terms of the notice of privacy practices in effect.

Questions and Contact Person for Requests
If you have any questions or want to make a request pursuant to the rights described above, please contact:
Office Manager
c/o Joseph McWherter, M.D.
709 West Leuda Street
Fort Worth, Texas 76104
(817) 926-2511 Phone
(817) 348-0638 Fax
This notice is effective on the following date: April 14, 2003

We may change our policies and this notice at any time and have those revised policies apply to all the protected health information we maintain. If or when we change our notice, we will post the new notice in the office where it can be seen.

Disclosures to Families and Loved Ones

This office honors the important role that families, friends, and other loved ones play in supporting our patients' health care and treatment. At the same time, we are committed to protecting our patients' privacy as well as complying with both state and federal law.

Accordingly, disclosure to other people, even family, must remain a decision that rests with the patient. To the extent that is possible, we will follow the alternatives addressed in this policy.

Policy

- This practice will comply with any patient's request for us to share their personal health information with family members(s) and other designated person(s). We will comply with their request as long as: 1) the oral request is noted in the patient's record (e.g. "at patient's request will share information with John Doe"), 2) the patient is competent to make this decision, and 3) the patient has not revoked that request. Note that revocations or limitations must also be documented in the patient's record.
- Patients who arrive at this office with others will be asked privately if they would like those persons present while they are being seen and/or treated.
- Patients who are undergoing procedures requiring anesthesia will be asked if they would like information shared with anyone prior to awakening.
- If the individual cannot express his/her request for sharing information, because of incapacity or an emergency circumstance, our physician(s) will exercise their professional judgment and determine whether the disclosure is in the best interest of the individual. If so, we will disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care.
- Patient's family members, neighbors, etc. that come to this office to pick up prescriptions. Equipment, directions, or other items associated with a patient's care will be permitted to do so if it is reasonable to infer they are involved with our patient's care.
- Notification of appropriate third parties also may occur without a patient's request or approval, to the extent this office is involved with disaster relief services, or acting in the role of notifying a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death.

Acknowledgement of Review of Notice of Privacy Practices

By my signature, I *(print name)* _____, acknowledge that I have reviewed this office's Notice of Privacy Practices, which explains how my medical information will be used and disclosed.

I understand that I am entitled to receive a copy of this document.

_____ _____

Signature of Patient or Personal Representative Date