Notice of Patients Rights and Privacy Protections under Federal Privacy Laws (HIPAA)

The Health Insurance Portability and Accountability Act of 2013, commonly referred to as HIPAA, requires this office to implement and maintain a number of policies and safeguards to insure that patients' protected health information (PHI) remains secure and only used in a manner consistent with HIPAA and similar laws.

General Rules and Definitions.

Protected Health Information, also referred to as PHI means any patiently identifiable health information, including demographic data, which relates to:

- the patient's past, present or future physical or mental health or condition,
- the provision of health care to the patient, or
- the past, present, or future payment for the provision of health care to the patient,

and identifies the patient or for which there is a reasonable basis to believe it can be used to identify the patient. Patiently identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

Covered Entity means: a) any health care provider, including this office, b) Health Plans, such as a health insurance company, an HMO, government health programs such as Medicare and Medicaid, c) a health care clearing house that processes nonstandard health information from one covered entity into a standard format, such as a billing agent.

Minimum Necessary. A central aspect of HIPAA is the principle of "minimum necessary" use and disclosure. This office will make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request. This office will develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, this office will not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose.

The minimum necessary requirement is not imposed in any of the following circumstances: (a) disclosure to or a request by a health care provider for treatment; (b) disclosure to an patient who is the subject of the information, or the patient's personal representative; (c) use or disclosure made pursuant to an authorization; (d) disclosure to HHS for complaint investigation, compliance review or enforcement; (e) use or disclosure that is required by law; or (f) use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules.

For the purposes of the minimum necessary requirement, the following employees/positions have the corresponding access to PHI:

Doctor or other health care provider who treats or directs treatment of patients: All PHI related to the patient under the doctor's care, or as the office's electronic billing/records system permits, necessary to diagnose, treat and perform other healthcare operations

Chiropractic Assistant or Chiropractic Technical Assistant (as certified by the state or Integrity Management): All PHI related to the patient under the doctor's care, or as

the office's billing/electronic records system permits necessary to treat and perform other healthcare operations.

Billing: All PHI as is minimally necessary to perform the duties of billing or obtain prior authorization of services, including, but not limited to, demographic information and doctor's notes, patients' medical history or as the office's electronic billing/records system permits.

Front Desk/Receptionist: All PHI as is minimally necessary to schedule appointments for patients and process patient's demographic and billing information or as the office's electronic billing/records system permits. This may include patients' demographic information, health care payer information, and statements made by the patient regarding their current or past medical condition.

Practice Representative: All PHI as is minimally necessary to schedule appointments for patients or as the office's electronic billing/records system permits.

We recognize that our office may have employees covering several positions on a temporary or permanent basis. Therefore the level of access to PHI shall be as necessary to perform the functions of the position.

Business Associate: In general, a Business Associate is defined by HIPAA as a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of patiently identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing. Business Associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. *However, persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all.* A covered entity can be the business associate of another covered entity.

Personal Representatives. HIPAA requires a this office to treat a *"personal representative"* the same as the patient, with respect to uses and disclosures of the patient's protected health information, as well as the patient's rights under the Rule.[84] A personal representative is defined by HIPAA as a person legally authorized to make health care decisions on an patient's behalf or to act for a deceased patient or the estate. HIPAA permits an exception when we has a reasonable belief that the personal representative may be abusing or neglecting the patient, or that treating the person as the personal representative could otherwise endanger the patient.

Special Case: Minors. In most cases, parents are the personal representatives for their minor children. Therefore, in most cases, parents can exercise patient rights, such as access to the medical record, on behalf of their minor children. In certain exceptional cases, the parent is not considered the personal representative. In these situations, HIPAA defers to State and other law to determine the rights of parents to access and control the protected health information of their minor children. If State and other law is silent concerning parental access to the minor's protected health information, our office has discretion to provide or deny a parent access to the minor's health information, provided the decision is made by a licensed health care professional, such as our doctor, in the exercise of professional judgment.

General Principles for Uses and Disclosures of PHI

Basic Principle. A major purpose of HIPAA is to define and limit the circumstances in which an patient's protected heath information may be used or disclosed by covered entities. This office may not use or disclose protected health information, except either: (1) as the HIPAA laws permits or requires; or (2) as the patient who is the subject of the information (or the patient's personal representative) authorizes in writing.

Any information that is disclosed should be the minimum amount of information necessary to accomplish the task, such as submitting a bill to an insurance company or obtaining a prior authorization.

Required Disclosures. This office must disclose protected health information in only two situations: (a) to patients (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to US Department of Health and Human Services when it is undertaking a compliance investigation or review or enforcement action.

Permitted Uses and Disclosures of PHI

Permitted Uses and Disclosures. This office is permitted to use and disclose protected health information, without an patient's authorization, for the following purposes or situations: (1) To the Patient (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purposes of research, public health or health care operations. We will rely on our professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

(1) To the Patient. This office may disclose protected health information to the patient who is the subject of the information.

(2) Treatment, Payment, Health Care Operations. This office may use and disclose protected health information for its own treatment, payment, and health care operations activities. We may also disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the patient and the protected health information pertains to the relationship.

a) ***Treatment*** is the provision, coordination, or management of health care and related services for a patient by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.

b) ***Payment*** encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an patient and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an patient.

c) Health care operations are any of the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance

functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.

In the unlikely event this office might, obtain, use or disclosure psychotherapy notes for treatment, payment, and health care operations purposes, we will require a written authorization from the patient prior to use or disclosure of the psychotherapy notes..

(3) Uses and Disclosures with Opportunity to Agree or Object. Informal permission may be obtained by asking the patient outright, or by circumstances that clearly give the patient the opportunity to agree, acquiesce, or object. Where the patient is incapacitated, in an emergency situation, or not available, this office may generally make such uses and disclosures, if in the exercise of our professional judgment, the use or disclosure is determined to be in the best interests of the patient.

Facility Directories. It is a common practice in many health care facilities, such as hospitals, to maintain a directory of patient contact information. A covered health care provider may rely on a patient's informal permission to list in its facility directory the patient's name, general condition, religious affiliation, and location in the provider's facility. The provider may then disclose the patient's condition and location in the facility to anyone asking for the patient by name, and also may disclose religious affiliation to clergy. Members of the clergy are not required to ask for the patient by name when inquiring about patient religious affiliation. We do not anticipate creating such a Facility Directory, but we need to advise you of the scope of the rule.

For Notification and Other Purposes. This office may also rely on a patient's informal permission to disclose to the patient's family, relatives, or friends, or to other persons whom the patient identifies, protected health information directly relevant to that person's involvement in the patient's care or payment for care. This provision, for example, allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient. Similarly, a covered entity may rely on an patient's informal permission to use or disclose protected health information for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the patient's care of the patient's location, general condition, or death. In addition, protected health information may be disclosed for notification purposes to public or private entities authorized by law or charter to assist in disaster relief efforts.

(4) Incidental Use and Disclosure. The Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated. A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is permitted as long as this office has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the "minimum necessary," as required by HIPAA.

(5) Public Interest and Benefit Activities. HIPAA permits use and disclosure of protected health information, without a patient's authorization or permission, for 12 national priority purposes. These disclosures are permitted, although not required, by the Rule in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, striking the balance between the patient privacy interest and the public interest need for this information. Those purposes are:

Required by Law. This office may use and disclose protected health information without patient authorization as required by law (including by statute, regulation, or court orders).

Public Health Activities. This office may disclose protected health information to: (1) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect; (2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance; (3) patients who may have contracted or been exposed to a communicable disease when notification is authorized by law; and (4) employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law..

Victims of Abuse, Neglect or Domestic Violence. In certain circumstances, this office may disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.[31]

Health Oversight Activities. This office may disclose protected health information to health oversight agencies, as defined by HIPAA, for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.

Judicial and Administrative Proceedings. This office may disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the patient or a protective order are provided.

Law Enforcement Purposes. This office may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.

Decedents. This office may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.

Cadaveric Organ, Eye, or Tissue Donation. This office may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.

Research. "Research" is defined by HIPAA as any systematic investigation designed to develop or contribute to generalizable knowledge. HIPAA permits this office to use and disclose protected health information for research purposes, without an patient's authorization,

provided the covered entity obtains either: (1) documentation that an alteration or waiver of patients' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board; (2) representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or (3) representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the patients about whom information is sought. A covered entity also may use or disclose, without an patients' authorization, a limited data set of protected health information for research purposes

Serious Threat to Health or Safety. This office may disclose protected health information that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). This office may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.

Essential Government Functions. An authorization is not required to use or disclose protected health information for certain essential government functions. Such functions include: assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.

Workers' Compensation. This office may disclose protected health information as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.

6) Limited Data Set. A limited data set is defined by HIPAAA as protected health information from which certain specified direct identifiers of patients and their relatives, household members, and employers have been removed. A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set.

Privacy Practices Notice. Our office, with certain exceptions, must provide a notice of its privacy practices. HIPAA that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must state our office's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must describe patients' rights, including the right to complain to HHS and to this office if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to our office. We must act in accordance with their notices. HIPAA also contains specific distribution requirements for direct treatment providers, all other health care providers, and health plans.

Notice Distribution. For every patient of our office, we must have delivered a privacy practices notice to patients starting April 14, 2003 as follows:

- Not later than the first service encounter by personal delivery (for patient visits), by automatic and contemporaneous electronic response (for electronic service

delivery), and by prompt mailing (for telephonic service delivery);
    - By posting the notice at each service delivery site in a clear and prominent place where people seeking service may reasonably be expected to be able to read the notice; and
    - In emergency treatment situations, the provider must furnish its notice as soon as practicable after the emergency abates.

We must also supply notice to anyone on request. Our office will also make its notice electronically available on any web site it maintains for customer service or benefits information.

- **Acknowledgement of Notice Receipt.** Our office must make a good faith effort to obtain written acknowledgement from patients of receipt of the privacy practices notice. HIPAA does not prescribe any particular content for the acknowledgement. The provider must document the reason for any failure to obtain the patient's written acknowledgement. The provider is relieved of the need to request acknowledgement in an emergency treatment situation.

Patient's Rights

Access. Except in certain circumstances, patients have the right to review and obtain a copy of their protected health information within 30 days of the request. HIPAA excepts from the right of access the following protected health information: psychotherapy notes, information compiled for legal proceedings, laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access, or information held by certain research laboratories. For information included within the right of access, our office may deny a patient access in certain specified situations, such as when a health care professional believes access could cause harm to the patient or another. In such situations, the patient must be given the right to have such denials reviewed by a licensed health care professional for a second opinion.

Electronic Access If your PHI is maintained in an electronic format, you have a right to an electronic copy of that information within 30 days of your request. If our system cannot readily provide it to you in your requested format, we will seek to agree upon a mutually acceptable format. As a last resort, we may have to provide you a paper copy.

Amendment. HIPAA gives patients the right to have covered entities amend their protected health information in a designated record set when that information is inaccurate or incomplete. If we accept an amendment request, it must make reasonable efforts to provide the amendment to persons that the patient has identified as needing it, and to persons that the covered entity knows might rely on the information to the patient's detriment. If the request is denied, covered entities must provide the patient with a written denial and allow the patient to submit a statement of disagreement for inclusion in the record. HIPAA specifies processes for requesting and responding to a request for amendment. We must amend protected health information in its designated record set upon receipt of notice to amend from another covered entity.

Disclosure Accounting. Patients have a right to an accounting of the disclosures of their protected health information by this office or our business associates. The maximum disclosure accounting period is the six years immediately preceding the accounting request, except a covered entity is not obligated to account for any disclosure made before its HIPAA compliance date.

HIPAA does not require accounting for disclosures: (a) for treatment, payment, or health care operations; (b) to the patient or the patient's personal representative; (c) for notification of or to persons involved in an patient's health care or payment for health care, for disaster relief, or for

facility directories; (d) pursuant to an authorization; (e) of a limited data set; (f) for national security or intelligence purposes; (g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or patients in lawful custody; or (h) incident to otherwise permitted or required uses or disclosures. Accounting for disclosures to health oversight agencies and law enforcement officials must be temporarily suspended on their written representation that an accounting would likely impede their activities.

Restriction Request. Patients have the right to request that this office restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in the patient's health care or payment for health care, or disclosure to notify family members or others about the patient's general condition, location, or death. Such requests should be documented in writing and maintained in the patient's record.

Restriction Request for Services Paid "Out-of-Pocket." Patients have the right to request that this office not disclose to a patient's health insurance company, HMO or other payer any PHI related to any treatment the patient has elected to pay "out-of-pocket." The patient must complete the "HIPAA REQUEST FOR NON-DISCOSURE OF PHI RELATING TO SERVICES PAID DIRECTLY BY PATIENT" form to document the request and should be maintained in the patient's record.

Confidential Communications Requirements. Our office must permit patients to request an alternative means or location for receiving communications of protected health information by means other than those that the covered entity typically employs. For example, an patient may request that we communicate with the patient through a designated address or phone number. Similarly, a patient may request that the provider send communications in a closed envelope rather than a post card. Such requests should be documented in writing and maintained in the patient's record.

Right to Revoke Authorization or Consent to Use PHI for Marketing or Fundraising Purposes. Patients have the right to revoke their consent or authorization to disclose or use their PHI for any fundraising or marketing purposes. The patient must complete the "HIPAA REVOCATION OF AUTHORIZATIONS OR CONSENT TO USE PHI FOR MARKETING OR FUNDRAISING PURPOSES" form to document the request and should be maintained in the patient's record. A list of all patients electing to opt out

The patient should be advised that they may still receive marketing and fundraising communications, but their name and other demographic information will have been derived from sources other than PHI, such as the White Pages or a community marketing list.

Sale of PHI. This office will not sell your PHI. However, we are legally required to inform you that if we were to sell your PHI, we must first y obtain your authorization.

Right to Revoke All Authorizations or Consent to Use or Disclose PHI. Patients have the right to revoke any or all authorizations to use or disclose PHI by this office. The patient must complete the "HIPAA REVOCATION OF ALL AUTHORIZATIONS OR CONSENT TO USE OR DISCLOSE PROTECTED HEALTH INFORMATION" form to document the request and should be maintained in the patient's record. The patient should be advised that this revocation may affect this office's ability to maintain the patient as a patient and treat them in the future.

Right to be Notified of a Breach. Patients have the right to be notified of a breach of the security of your PHI, unless there is a low probability your PHI has been compromised.

Administrative Requirements

HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the flexibility and scalability of the Rule are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources.

Privacy Policies and Procedures. A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.[64]

Privacy Personnel. Our office has designated Stephen E. Thomas, DC as our Privacy Official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing patients with information on this office's privacy practices.

Mitigation. We must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.

Data Safeguards. This office must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of HIPAA and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. Our office shall practice to ensure reasonable safeguards for patients' health information – for instance:

- By speaking quietly when discussing a patient's condition with family members in a waiting room or other public area;
- By avoiding using patients' names in public hallways and elevators, and posting signs to remind employees to protect patient confidentiality;
- By isolating or locking file cabinets or records rooms; or
- By providing additional security, such as passwords, on computers maintaining personal information

Documentation and Record Retention. Our office will maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that HIPAA requires to be documented.

Changes to this Notice. We reserve the right to change this notice. Any changes contained in the new notice will apply to Health Information already in the possession of our office as well as any information we receive in the future. A current copy of the notice will be posted in the office and on our website, if we have a website.

Complaints

Complaints. Any complaints regard our privacy policies or procedures should be directed to our Privacy Officer, who is Stephen E. Thomas, DC.

Retaliation and Waiver. This office will not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule. Our office will not require a patient to waive any rights not under HIPAA as a condition for obtaining treatment.