**HIPAA Privacy Plan**

**Policies and Procedures**

**Section 1: Introduction to HIPAA Privacy Policies and Procedures**

This training is to help you understand our HIPAA compliance policies and procedures. You are responsible to adhere to each of the principles presented in this training

The goals of this training are:

As an employee you are bound by the privacy rule and can only have access to protected health information on a need to know basis to perform your job.

**HIPAA Definition**

HIPAA stands for Health Insurance Portability and Accountability Act

**PHI Definition**

PHI stands for Protected Health Information

**Notice of Privacy Practices**

**Policy**

The notice of privacy practices (NPP) is a statement from our office to the patient about how his or her PHI is handled and protected by us. It is only a notice and not an authorization. We provide the NPP to our patients.

**Procedure**

We provide the NPP to the patient on or before the first delivery of service, except in an emergency situation. We obtain, once for each patient (or parent or legal guardian), a signed acknowledgment that they have received a copy of the NPP. We then place the signed acknowledgment in the patient's chart. If the patient refuses to sign the acknowledgment, we document on that acknowledgment that the patient was given an NPP and refused to sign the form. Then we place that noted acknowledgment form in the patient's chart. Treatment does not depend on a signed acknowledgment of receipt of the NPP.

**Business Associates**

**Policy**

We obtain business associate agreements from all whom we hire or work with to handle PHI on our behalf. We disclose PHI to our Business Associates only after we obtain business associate agreements.

**Procedure**

We obtain a business associate agreement or contract from all Business Associates. We may disclose PHI to a business associate for purposes agreed to by contract. Our business associates are required to be independently compliant with HIPAA privacy and security, as well as the breach notification and requirements of HIPAA HITECH.

**Retention of Records**

**Policy**

We retain all PHI and HIPAA related documents for six years.

**Procedure**

We retain all HIPAA related documents for six years as required by law. This applies to: any patient information, signed or noted NPP acknowledgements, forms used in HIPAA related transactions, etc.

We destroy these records by burning or shredding to ensure that there is no allowance for disclosure of any PHI. This retention does not apply to medical records

**Uses and Disclosures of PHI for Treatment, Payment, or Health Care Operations (TPO)**

**Policy**

Our office uses and/or discloses PHI for TPO purposes without the patient's signed authorization.

**Procedure**

Our office uses and/or discloses PHI for TPO purposes without the patient signed authorization in the following examples:

**Required Uses and Disclosure of PHI Without an Authorization**

**Policy**

Our office uses and/or discloses PHI without the patient signed authorization when required or allowed by law.

**Procedures**

There are several circumstances, other than for TPO purposes, under which the patient's signed authorization is not required for uses and disclosures of PHI when allowed by law. The most common are:

* Other medical providers participating in the patient’s treatment
* Diagnostic labs/imaging centers
* Medical billing companies billing for services performed

**Authorization**

**Policy**

Our office requires signed patient authorizations for non-TPO uses and disclosures of PHI.

**Procedure**

We require patient authorization for non-TPO uses and disclosures of PHI. An authorization is a customized document that gives our practice permission to use specified PHI for specified purposes.

If we become aware that patient information is ever disclosed incidentally or accidentally without an authorization for purposes other than TPO, we are required to contact the compliance officer immediately.

**Use of PHI: Restriction for Use and Disclosure of PHI**

**Policy**

Our patients have the right under HIPAA Privacy rules to request a restriction on certain types of uses and disclosure of their protected health information.

**Procedure**

When a patient requests a restriction, we use our "request for restrictions disclosure of PHI" form. We may deny individuals request for a restriction, but we make sure we have defensible grounds for the denial.

We must honor a patient's request to restrict the use and disclosure of their PHI to a health plan for payment purposes if the patient has paid for those particular services infull.

**Use of PHI: Minimum Necessary**

**Policy**

Our office has determined our own set of standards for minimum necessary use and disclosure of PHI. This determination and training in its application is the responsibility of the HIPAA compliance officer. Our office adheres to a standard for "minimum necessary" use and disclosure of PHI.

**Procedure**

HIPAA requires that our practice adhere to a standard for "minimum necessary" use and disclosure of PHI. We make reasonable efforts to limit the use of, the disclosure of, and the request for PHI to the minimum necessary to accomplish the intended purpose of any request. HHS requires that we determine our own set of standards for minimum necessary use and disclosure of PHI. This determination and training in its application is the responsibility of the HIPAA compliance officer.

**Use of PHI: Reasonable Reliance**

**Policy**

When a request for patient information is seeking more than the minimum necessary PHI, we will limit the disclosure to the minimum deemed necessary.

**Procedure**

When the request for patient information is seeking more than the minimum necessary PHI, the privacy rule requires us to limit the disclosure to the minimum we think is necessary using a reasonable effort to limit patient information while providing the best care for the patient. However, if another treatment provider requests the disclosure of PHI, we may reasonably assume that the request is for the minimum necessary for their purpose. In turn, when our practice is requesting PHI from another provider, we must determine what the minimum necessary is for our own request purposes.

**Use of PHI: Accounting for Uses and Disclosures**

**Policy**

The patient has the right to request an accounting of all non-TPO disclosures of their PHI

**Procedure**

The patient has the right to request an accounting of all non-TPO disclosures of his or her PHI. The patient must request this accounting on our "request for a count of disclosures of PHI" form. When PHI is disclosed for a non-TPO purpose, it must be documented on a patient's "report of PHI disclosures" form and placed into the patient's digital chart. Use this log as a record of the disclosures.

**Use of PHI: Mitigation**

**Policy**

If we accidentally disclose PHI for any reason that is not allowed or required under the privacy rule, and that disclosure is apt to cause harm to the patient, the HIPAA compliance officer must inform the patient of the disclosure.

**Procedure**

If we accidentally disclose PHI for a reason that is not allowed or required under the Privacy Rule and that disclosure is apt to cause harm to the patient, the HIPAA Compliance Officer must inform the patient of the disclosure. The HIPAA Compliance Officer also must take action necessary to repair the harm done by the disclosure and promptly change the office procedures that allowed the disclosure to occur. This type of disclosure needs to be accounted for on the disclosure logs.

**Use of PHI: Faxes and E-mail**

**Policy**

It is our responsibility to make sure that faxes and e-mails from our office automatically include an adequate privacy warning.

**Procedure**

It is our responsibility to make sure that faxes and e-mails from our office are automatically including an adequate privacy warning. We use the following example:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Privileged and confidential: this document and the information contained herein are confidential and protected from disclosure pursuant to federal law. This message is intended only for the use of the Addressee(s) and may contain information that is privileged and confidential. If you are not the intended recipient, you are hereby notified that the use, dissemination, or copying of this information is strictly prohibited. If you received this communication in error, please erase all copies of the message and its attachments and notify the sender immediately.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Section 2: Safeguards**

**Reasonable Safeguards**

**Policy**

We protect our patients PHI with reasonable safeguards

**Procedure**

We protect our patients’ PHI by:

Having locks on our file room doors

Having ‘employees only’ signs in specific areas

Not discussing patient care on social media

Proper billing to proper carriers

Shredding unnecessary documents or notes that have patient information on them

Placing working items with patient PHI in areas that can’t be seen by through traffic

**Oral Communications**

**Policy**

We are extremely cautious when speaking in our office

**Procedure**

We are extremely cautious when speaking in our office. In any conversation, we are certain that our voice was lowered and that we discussed only the "Minimum Necessary" information. Calling out the patient's name in the waiting room or elsewhere in our practice is not considered disclosing PHI, as long as the name only as mentioned, but not any other direct identifiers such as address, telephone number, Social Security number, or reason for the visit.

**Sign-in Sheets**

**Policy**

We provide sign-in sheets for our patients to sign when they arrive for their appointments.

**Procedure**

We provide sign in sheets, which are permitted by the privacy rule as long as the only information listed on them is the minimum necessary information. Sign-in sheets can only include the doctor’s name, patient's name, appointment time, and patient's time of arrival for the appointment. Other identifying information is prohibited. We allow no PHI on the sign in sheet.

**Call Verification**

**Policy**

We verify the identity of those to whom we speak on the telephone with any PHI is discussed during the call. This is done to ensure that the caller is the patient. We do not disclose any more than the minimum necessary during phone conversations unless we have authorization either by law or from the patient to disclose the information.

**Procedure**

When answering the phone, we make certain the person you're speaking to is identified properly.

**Phone Messages and Appointment Reminders**

**Policy**

When we call our patients to leave any kind of message, and we encounter an answering machine or talk to another person, we do not leave any more than the minimum necessary or approved PHI in the message.

**Procedure**

If we're calling the patient about test results, we may leave a message with a family member or on their answering machine, but we may only leave the name of the doctor, our phone number, and request a return call. We cannot leave test results, the reason for the appointment, or any instructions about the appointment unless we have the signed authorization permitting a specific person to receive the information. That person must then be properly identified.

**Phone Appointments and Reminder Cards**

**Policy**

If we send appointment reminder cards to our patients, we limit the information on the cards to the "minimum necessary", and they contain No PHI.

**Procedure**

Reminder cards can be sent out, but must be limited to the "minimum necessary" and contain no PHI. We may list on the card patient's name, date, and time of the appointment, but not the reason for the appointment. We may also leave messages on answering machines, and may leave only the name and phone number of our practice and that we would like the person to return the call, or an appointment reminder.

**Visitors**

**Policy**

We prevent unauthorized individuals from access to areas in our office that are a source of patient information, whether verbal, written, or electronic. Unauthorized visitors have access only to areas directly related to their jobs, but not to PHI.

**Procedure**

Anyone that we cannot identify as a person with a valid reason for being in our office, should be reported to the HIPAA Compliance Officer immediately. Authorized visitors have access only to areas directly related to their jobs, but not PHI. Authorized visitors must sign the visitors log and should be accompanied by an employee. Incidental disclosures to these people can happen and are allowed as long as our office is applying the minimum necessary and reasonable safeguard standards. Family members can accompany patients when the patient approves.

The HIPAA Privacy Rule specifically addresses the need to prevent unauthorized individuals from access to areas in our office that are a source of patient information, whether verbal, written or electronic. These individuals might include supplier representatives, office machine repair personnel, janitorial service workers, etc. If you are applying the minimum necessary standard and reasonable safeguards, any disclosure of PHI to these visitors are considered incidental disclosures. These visitors are not considered business associates.

This does not include family members who accompanied the patient and are involved in the patient's medical care.

**Handling Explanations of Benefits**

**Policy**

When we send a copy of the primary insurance Explanation of Benefits (EOB) to the patients secondary insurance, we black-or-white out the PHI that does not apply to the claim.

**Procedure**

During the course of billing a secondary insurance carrier, we send a copy of the primary insurance Explanation of Benefits. There may be other patients PHI on the EOB. We make sure to black or white out the PHI that does not apply to the claim.

**Auditing**

**Policy**

We audit a randomly selected group of patient records on a semiannual basis.

**Procedure**

The Compliance Officer audits a randomly selected group of patient records. This procedure is performed semiannually. We use our audit forms to perform billing and privacy audits and to check for HIPAA violations.

**Distraction of PHI**

**Policy**

We properly destroy all PHI to ensure that it does not have the potential of being disclosed wrongfully.

**Procedure**

HIPAA law requires that all HIPAA related records and documents are retained for six years (paper and electronic). This applies to authorizations, arbitration records, and business associate agreements, even if lapsed.

If either paper or electronic files (including hard or soft discs) are disposed of, we make certain they are erased, shredded, or disposed of properly so they do not have the potential of being disclosed wrongfully. We are responsible for any wrongful disclosures resulting from failure to properly destroy PHI.

**Patient Access: Patient's Right of Access**

**Policy**

Patients have the right to access their PHI maintained in a designated record set by our office.

**Procedure**

Our patients have the right to access their PHI. To access their PHI, the patient needs to complete a "request to inspect or copy protected health information" form. HIPAA provides all individuals with the right to access their PHI maintained by our office and by other health care providers who create or receive their PHI.

**Patient Access: Access for Personal Representatives**

**Policy**

We acknowledge that individuals have the right to obtain access to, and to request amendments to, health information about them. These rights also rest with the "personal representative" of that individual, for the parents of an un-emancipated minor and for deceased individual’s representative.

**Procedure**

Our office acknowledges that individuals have the right to obtain access to, and to request amendment to, health information about them. These rights also rest with the "personal representative" of that individual, for the parents of an un-emancipated minor, and for a deceased individual’s representative. A personal representative has the same right and authority as the patient. A person is been legally designated (legal guardian, executor of will, next of kin, power-of-attorney, etc.) to represent a patient is also referred to as a "personal representative" of the patient.

**Patient access: Minor Children**

**Policy**

In our office, minor children must always be accompanied by a parent or legal guardian to receive treatment, except in emergency situations or where the parent has written a waiver from attending. The parent or legal guardian generally has access to the child's medical records.

**Procedure**

Although a parent or legal guardian should always accompany minor children, we may treat minor children in an emergency situation without a parent or guardian present. The parent or guardian is still entitled access to medical records, unless in the use of professional judgment our physician suspects abuse, neglect, or reasonably believes that releasing the information to the parent would endanger the child.

**Fees for Copying**

**Policy**

We charge a reasonable fee for our costs associated with the copying of medical records. We do not charge for the retrieval time of those records.

**Procedure**

HIPAA allows us to charge a reasonable fee for our costs associated with the copying of medical records. We may not charge for the retrieval time.

**Amending Patient Records**

**Policy**

We acknowledge that patients have the right to request amendments to their medical records. They do not have the right to change any information within their record.

**Procedure**

In our office patients have the right to request amendments to their medical records. The patient must complete a "Request to Amend Patient Records" form. Patient’s do not have the right to change any information within their record, but they can submit a written amendment to any part of the record. We may deny the individual's request for amendment, but we must make sure we have defensible grounds for the denial.

**Patient's Right to Request Confidential Communication**

**Policy**

A patient has the right to request that our office communicate with him or her in a specific manner, time, and place.

**Procedure**

A patient has the right to request that our office communicate with him or her in a specific manner, time, and place. The patient must complete a request for confidential communication form.

**Legal issues: Abuse and Neglect**

**Policy**

Cases of abuse and neglect are very serious issues. We are permitted by law to report cases of abuse and neglect.

**Procedure**

We report suspected cases of abuse and neglect because it is allowable under HIPAA regulations. They are very serious issues and need to be handled properly. Laws for reporting suspected cases of abuse and neglect are stringent. If we suspect a case of abuse or neglect, we will contact our HIPAA Compliance Officer at once.

**Legal issues: Privacy Complaints**

**Policy**

The Office for Civil Rights (OCR) has a legal responsibility to investigate every official privacy complaint they receive. Our office responds to privacy complaints in our office with an official inquiry.

**Procedure**

The Office for Civil Rights (OCR) has stated that they have a legal responsibility to investigate every official privacy complaint they receive. We may not require individuals to waive their rights to file a complaint as a condition of treatment or payment. Any complaints of HIPAA violations are the responsibility of your HIPAA Compliance Officer. We use the official "TCS Complaint form" and send it to the office for civil rights when required. It our policy not to retaliate on anyone making a complaint.

**Legal Issues: Public Health**

**Policy**

We disclose to the proper authorities PHI that specifically may affect the public health.

**Procedure**

We disclose PHI that may affect public health to the proper authorities authorized by law to collect such information.

**Legal Issues: Workers Compensation**

**Policy**

Workers compensation is not covered under the rules and regulations of HIPAA. State law governs use and disclosure of PHI for Workers Compensation claims.

**Procedure**

The Privacy Rule permits us to disclose PHI to workers compensation insurers, State administrators, employers, self-insured compensation plans, and other persons involved in workers compensation, without the authorization of the individual. However the disclosure must be required by law or needed for payment reasons.

**Legal Issues: Subpoenas**

**Policy**

We are permitted by law to respond to a subpoena request after receiving "satisfactory assurances".

**Procedure**

If our office receives a subpoena, our HIPAA Compliance Officer will make sure that we have received "satisfactory assurances" that the person about whom the subpoena has been issued has been notified.

**Legal Issues: Police and Law Enforcement**

**Policy**

We disclose PHI to law enforcement under certain circumstances.

**Procedure**

The Privacy Rule established new procedures and safeguards to restrict the circumstances under which we may give information to law enforcement officers. We may disclose information to law enforcement, absent a warrant or other prior process, when law enforcement is seeking to identify or locate a suspect.

**Workforce Members: Training**

**Policy**

We acknowledge that both ongoing and annual training is required of covered entities and business associates to maintain ongoing compliance to changing laws.

**Procedure**

We train our workforce on an annual basis. The Government has said that ongoing training is required of covered entities to maintain ongoing compliance. There will be changes in HIPAA that will require this annual training. It is the responsibility of the HIPAA Compliance Officer to ensure that all members of the practice participate in training and place an updated training law in the manual.

**Workforce Members: Employment Records**

**Policy**

We keep our employees PHI separate from their employment records.

**Procedure**

When an employee authorizes disclosure of PHI to his employer to substantiate sick leave, etc., those records then become a part of the employment record and are no longer considered PHI. The employment records of our employees are always kept completely separate from their medical records.

**Transactions and Code Sets**

**EDI Transactions/Implementation Guides**

**Policy**

We obtain from our software vendor and electronic clearinghouse, documentation that they comply with the HIPAA TSC standard.

**Procedure**

To be compliant with the electronic HIPAA Transaction and Code Sets Standard (TCS), we must obtain from our software vendor and electronic clearinghouse documentation that they comply with HIPAA TCS standard.

**Transactions and Code Sets: Medical Code Sets**

**Policy**

It is our policy to consistently assign the most current and accurate code sets when documenting the billing for services provided to our patients.

**Procedure**

To describe diseases, syndromes or conditions presented by our patients we always use the most current and accurate ICD-9-CM diagnosis codes.

To describe the procedures, supplies and services we provide to our patients, we always use the most current and accurate CPT and HCPCS codes.