HIPAA Privacy Policy & Notice of Privacy Practices

1. PURPOSE

The purpose of this policy is to comply with patient personal health information security rights and privacy regulations as outlined in the Health Information Portability and Accountability Act.

2. SCOPE

a. This policy applies to all organization's employees, management, contractors, student interns, and volunteers.
b. This policy describes the organization's objectives and policies regarding maintaining the privacy of patient information.

3. POLICIES, PROCEDURES AND STATEMENTS

a. All Premier employees must sign a HIPPA privacy agreement prior to starting employment
b. All paperwork prepared or collected for a patient is private and is not to be shared with anyone not directly involved with creating a Premier medical billing invoice for the tests performed except; a copy may be made for the interpreting physician who may be a part of the client practice or an outside service designated by the client practice.
c. Sonographers and office assistants will use appropriate safeguards with daily schedules and log sheets and keep them in a location not accessible to patients.
d. No employees or business associates shall discuss any tests scheduled or the results with anyone not directly involved with a patient's medical care.
e. Patient paperwork will be held in a secure location only accessible to Premier personnel.
f. Patient paperwork may only be mailed in secure envelopes and addressed to a specific person at client practices, interpreting physicians, patient designated health plans or Premier personnel.
g. Patient paperwork may only be faxed to a specific person at Client Practices, Interpreting Physicians, Patient Designated Health Plans and Premier personnel.
h. Any paperwork that contains patient information not being retained for billing purposes must be shredded or placed in a secure burn box for proper disposal.
i. All computers storing patient information shall be accessible only by authorized login names and passwords approved by the Executive Management or Privacy Official. Inactive logins and passwords will be deleted immediately upon termination of employment or contract.
j. All computers containing patient health information will be secured at Premier, Business Associate or Client Practice facilities.

4. RESPONSIBILITIES

a. President

1) Establish program objectives
2) Approve privacy policy
3) Provide training for work force
4) Enforce sanctions
5) Designate Privacy Official(s)

b. Privacy Official (s)

1) Develops privacy policies and procedures
2) Provides administrative and physical safeguards and coordinates and implements privacy policy and procedures through organization's departments
3) Develops, implements and documents the privacy training program as described in Section 11 of this policy
4) Ensure employees sign HIPPA privacy agreement
5) Receives and processes privacy complaints
6) Processes individual rights requests including patients:

a) Right to access/copy protected health information (PHI)
b) Right to amend PHI
c) Right to restrict use/disclosure
d) Right to confidential communications
e) Right to an accounting of disclosures
f) Right to file a complaint

7) Ensures retention of HIPAA policies and procedures, complaints, and investigative materials to meet compliance requirements.
8) Processes Business Associate Agreements (BAA)

a) Conducts Business Associate Agreements inventory
b) Develops and coordinates Business Associate Agreement template
c) Conducts annual review/update

c. Employee responsibilities

1) Understand and comply with organization's policies regarding patient confidentiality and privacy

5. DESIGNATED RECORD SET

a. Billing Offices Paper Documents
b. Client Practice Exam Rooms/Offices Paper Documents
c. Billing Offices Computerized Data
d. Client Practice Exam Rooms/Offices Computerized Data
e. Business Associates Paper Documents
f. Business Associates Paper Documents Computerized Data

6. NOTICE OF PRIVACY PRACTICES (NPP) (SEE ADDENDUM)

a. The Notice of Privacy Practices will be posted and maintained on the company's website at all times.

7. MINIMUM NECESSARY POLICY

Premier will only disclose a patient's health information record:

a. To the patients designated health plan.
b. To patients designated physicians.
c. As required by law.
d. To employees/business associates of Premier as required for treatment, payment or healthcare operations.

8. USE AND/OR DISCLOSURE OF PROTECTED HEALTH INFORMATION (see addendum)

a. A description of how Premier may use and disclose protected health information can be found in the Addendum attached "Notice of Privacy Practices" NPP.

9. SAFEGUARDS FOR THE PROTECTION OF PHI

a. Require individual logins and passwords to computers
b. Shred or burn unneeded patient health information
c. deny access to non-employee/ business associates to patient health information
d. lock facilities containing patient health information when unattended
e. mail or fax patient health information only to individually addressed authorized personnel of Premier, patient's designated health plan or patient physician offices.

10. WORK FORCE TRAINING

a. Premier's Privacy Officer will ensure that initial and recurrent training regarding patient health information is performed and reinforced periodically.
f. Training will include but not limited to; safeguarding physical documents, safeguarding logins and passwords, identity verification before any phone or mail disclosure, proper document disposal.

11. BUSINESS ASSOCIATE AGREEMENTS

a. Premier's Privacy Officer will ensure that all contractors and third party providers have signed Premier's current Business Associate Agreement.

12. EMPLOYEE COMPLAINTS

a. The Privacy Officer will respond immediately to any employee/business associate generated privacy complaints and will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals who exercise any right under the HIPAA privacy rule, including filing a complaint.

13. SANCTIONS

a. Disciplinary action for the first unintentional violation of Premier privacy policies will include verbal counseling and remedial training. Further violations may include termination depending on circumstances. Intentional violations of Premier privacy policies will result in immediate termination.

I acknowledge that I have received the Premier Diagnostic Services, Inc. HIPPA PRIVACY POLICY & NOTICE OF PRIVACY PRACTICES and that I have read and understand the policy.

_____

EMPLOYEE SIGNATURE DATE

ADDENDUM

PREMIER DIAGNOSTIC SERVICES, INC

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 Notice of Privacy Practices describes how we may use and disclose your protected health information to carry out treatment, payment or health care operations and for other purposes that are permitted or required by law. It also describes your rights to access and control your protected health information. "Protected health information" is information about you, including demographic information, that may identify you and that relates to your past, present or future physical condition and related health care services.

We are required to abide by the terms of this Notice of Privacy Practices. We may change the terms of our notice, at any time. The new notice will be effective for all protected health information that we maintain at that time. Upon your request, we will provide you with any revised Notice of Privacy Practices. You may request a revised version by accessing our website, or calling the office and requesting that a revised copy be sent to you in the mail or asking for one at the time of your next appointment.

1. USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

Your protected health information may be used and disclosed by your physician, our office staff and others outside our office that are involved in your care and treatment for the purpose of providing health care services to you. Your protected health information may also be used and disclosed to pay your health care bills and to support the operation of your physician's practice.

Following are examples of the types of uses and disclosures of your protected health information that your physician's office is permitted to make. These examples are not meant to be exhaustive, but to describe the types of uses and disclosures that may be made by our office.

Treatment: We will use and disclose your protected health information to provide, coordinate, or manage your health care and any related services. This includes the coordination or management of your health care with another provider. For example, we would disclose your protected health information, as necessary, to a home health agency that provides care to you. We will also disclose protected health information to other physicians who may be treating you. For example, your protected health information may be provided to a physician to whom you have been referred to ensure that the physician has the necessary information to diagnose or treat you. In addition, we may disclose your protected health information from time-to-time to another physician or health care provider (*e.g.*, a specialist or laboratory) who, at the request of your physician, becomes involved in your care by providing assistance with your health care diagnosis or treatment to your physician.

Payment: Your protected health information will be used and disclosed, as needed, to obtain payment for your health care services provided by us or by another provider. This may include certain activities that your health insurance plan may undertake before it approves or pays for the health care services we recommend for you such as: making a determination of eligibility or coverage for insurance benefits, reviewing services provided to you for medical necessity, and undertaking utilization review activities. For example, obtaining approval for a hospital stay may require that your relevant protected health information be disclosed to the health plan to obtain approval for the hospital admission.

Health Care Operations: We may use or disclose, as needed, your protected health information in order to support the business activities of your physician's practice. These activities include, but are not limited to, quality assessment activities, employee review activities, training of medical students, licensing, fundraising activities, and conducting or arranging for other business activities.

We will share your protected health information with third party "business associates" that perform various activities (for example, billing or transcription services) for our practice. Whenever an arrangement between our office and a business associate involves the use or disclosure of your protected health information, we will have a written contract that contains terms that will protect the privacy of your protected health information.

We may use or disclose your protected health information, as necessary, to provide you with information about treatment alternatives or other health-related benefits and services that may be of interest to you. You may contact our Privacy Officer to request that these materials not be sent to you.

Other Permitted and Required Uses and Disclosures That May Be Made Without Your Authorization or Opportunity to Agree or Object

We may use or disclose your protected health information in the following situations without your authorization or providing you the opportunity to agree or object. These situations include:

Required By Law: We may use or disclose your protected health information to the extent that the use or disclosure is required by law. The use or disclosure will be made in compliance with the law and will be limited to the relevant requirements of the law. You will be notified, if required by law, of any such uses or disclosures.

Public Health: We may disclose your protected health information for public health activities and purposes to a public health authority that is permitted by law to collect or receive the information. For example, a disclosure may be made for the purpose of preventing or controlling disease, injury or disability.

Communicable Diseases: We may disclose your protected health information, if authorized by law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease or condition.

Health Oversight: We may disclose protected health information to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs and civil rights laws.

Abuse or Neglect: We may disclose your protected health information to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, we may disclose your protected health information if we believe that you have been a victim of abuse, neglect or domestic violence to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

Food and Drug Administration: We may disclose your protected health information to a person or company required by the Food and Drug Administration for the purpose of quality, safety, or effectiveness of FDA-regulated products or activities including, to report adverse events, product defects or problems, biologic product deviations, to track products; to enable product recalls; to make repairs or replacements, or to conduct post marketing surveillance, as required.

Legal Proceedings: We may disclose protected health information in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized), or in certain conditions in response to a subpoena, discovery request or other lawful process.

Law Enforcement: We may also disclose protected health information, so long as applicable legal requirements are met, for law enforcement purposes. These law enforcement purposes include (1) legal processes and otherwise required by law, (2) limited information requests for identification and location purposes, (3) pertaining to victims of a crime, (4) suspicion that death has occurred as a result of criminal conduct, (5) in the event that a crime occurs on the premises of our practice, and (6) medical emergency (not on our practice's premises) and it is likely that a crime has occurred.

Criminal Activity: Consistent with applicable federal and state laws, we may disclose your protected health information, if we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. We may also disclose protected health information if it is necessary for law enforcement authorities to identify or apprehend an individual.

Military Activity and National Security: When the appropriate conditions apply, we may use or disclose protected health information of individuals who are Armed Forces personnel (1) for activities deemed necessary by appropriate military command authorities; (2) for the purpose of a determination by the Department of Veterans Affairs of your eligibility for benefits, or (3) to foreign military authority if you are a member of that foreign military services. We may also disclose your protected health information to authorized federal officials for conducting national security and intelligence activities, including for the provision of protective services to the President or others legally authorized.

Workers' Compensation: We may disclose your protected health information as authorized to comply with workers' compensation laws and other similar legally-established programs.

Inmates: We may use or disclose your protected health information if you are an inmate of a correctional facility and your physician created or received your protected health information in the course of providing care to you.

Uses and Disclosures of Protected Health Information Based upon Your Written Authorization

Other uses and disclosures of your protected health information will be made only with your written authorization, unless otherwise permitted or required by law as described below. You may revoke this authorization in writing at any time. If you revoke your authorization, we will no longer use or disclose your protected health information for the reasons covered by your written authorization. Please understand that we are unable to take back any disclosures already made with your authorization.

Other Permitted and Required Uses and Disclosures That Require Providing You the Opportunity to Agree or Object

We may use and disclose your protected health information in the following instances. You have the opportunity to agree or object to the use or disclosure of all or part of your protected health information. If you are not present or able to agree or object to the use or disclosure of the protected health information, then your physician may, using professional judgement, determine whether the disclosure is in your best interest.

Facility Directories: Unless you object, we will use and disclose in our facility directory your name, the location at which you are receiving care.

2. YOUR RIGHTS

Following is a statement of your rights with respect to your protected health information and a brief description of how you may exercise these rights.

You have the right to inspect and copy your protected health information. This means you may inspect and obtain a copy of protected health information about you for so long as we maintain the protected health information. You may obtain your medical record that contains medical and billing records and any other records that your physician and the practice uses for making decisions about you. As permitted by federal or state law, we may charge you a reasonable copy fee for a copy of your records.

Under federal law, however, you may not inspect or copy the following records: psychotherapy notes; information compiled in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding; and laboratory results that are subject to law that prohibits access to protected health information. Depending on the circumstances, a decision to deny access may be reviewable. In some circumstances, you may have a right to have this decision reviewed. Please contact our Privacy Officer if you have questions about access to your medical record.

You have the right to request a restriction of your protected health information. This means you may ask us not to use or disclose any part of your protected health information for the purposes of treatment, payment or health care operations. You may also request that any part of your protected health information not be disclosed to family members or friends who may be involved in your care or for notification purposes as described in this Notice of Privacy Practices. Your request must state the specific restriction requested and to whom you want the restriction to apply.

Your physician is not required to agree to a restriction that you may request. If your physician does agree to the requested restriction, we may not use or disclose your protected health information in violation of that restriction unless it is needed to provide emergency treatment. With this in mind, please discuss any restriction you wish to request with your physician. You may request a restriction by contacting our Privact Office at the number designated below.

You have the right to request to receive confidential communications from us by alternative means or at an alternative location. We will accommodate reasonable requests. We may also condition this accommodation by asking you for information as to how payment will be handled or specification of an alternative address or other method of contact. We will not request an explanation from you as to the basis for the request. Please make this request in writing to our Privacy Officer.

You may have the right to have your physician amend your protected health information. This means you may request an amendment of protected health information about you in a designated record set for so long as we maintain this information. In certain cases, we may deny your request for an amendment. If we deny your request for amendment, you have the right to file a statement of disagreement with us and we may prepare a rebuttal to your statement and will provide you with a copy of any such rebuttal. Please contact our Privacy Officer if you have questions about amending your medical record.

You have the right to receive an accounting of certain disclosures we have made, if any, of your protected health information. This right applies to disclosures for purposes other than treatment, payment or health care operations as described in this Notice of Privacy Practices. It excludes disclosures we may have made to you if you authorized us to make the disclosure, for a facility directory, to family members or friends involved in your care, or for notification purposes, for national security or intelligence, to law enforcement (as provided in the privacy rule) or correctional facilities, as part of a limited data set disclosure. You have the right to receive specific information regarding these disclosures that occur after April 14, 2003. The right to receive this information is subject to certain exceptions, restrictions and limitations.

You have the right to obtain a paper copy of this notice from us, upon request, even if you have agreed to accept this notice electronically.

3. COMPLAINTS

You may complain to us or to the Secretary of Health and Human Services if you believe your privacy rights have been violated by us. You may file a complaint with us by notifying our Privacy Officer of your complaint. We will not retaliate against you for filing a complaint.

You may contact our Privacy Officer at (800)346-2111 for further information about the complaint process.

This notice was published and becomes effective on DECEMBER 2003**.**