

# HIPAA Privacy Policies

---

These policies describe Premier Primary Care's adherence to patient privacy, as required by the Health Insurance Portability and Accountability Act.

## Release of Patient Information – Patient Access

All information contained within a patient's medical record or within computerized systems of this practice will be maintained in a confidential manner to protect the patient's right to confidentiality and comply with city, state and federal regulations including HIPAA.

We honor a patient's written request to send medical information to another provider, hospital, medical facility, to an attorney, insurance practice and directly to the patient.

Protected Health Information (PHI) may only be accessed or released as follows:

- Directly to the Patient, upon request;
- To those directly involved in the care of the patient;
- For the protection of public health as provided by law;
- For the payment of services as authorized by the patient;
- To assist researchers, but only as authorized by the patient;

Protected Health Information may be released only if the authorization from the patient is:

- In writing, dated and signed;
- Specifies the information to be disclosed;
- Specifies the individual or location requiring the information;
- Specifies the contact person receiving the information.

### *Procedures*

The following procedures apply to the release of information:

- Patients must complete an Authorization to Release Protected Health Information form.
- Attorneys requesting medical records are required to have the patient complete power of attorney and approved Authorization to Release Protected Health Information form.
- The signature on the Authorization to Release Protected Health Information form should be reviewed to assure that it matches the documentation in the medical record.
- The date on the authorization must be no more than 60 days old.
- In an emergency situation, a healthcare provider can provide medical information to a physician, hospital, or medical facility upon receipt of the faxed required authorization on the letterhead of the organization indicating that the patient is unable to sign.
- Medical information can be released to a physician who refers a patient for a specialty consult. The report of their findings will be sent to the referring physician.
- Medical information can be provided to a homecare agency when referring a patient to a homecare agency.

- Medical records will be copied and forwarded within 3 business days of receipt of a written request for such information.

### ***Research***

Should this practice participate in a research study, the staff members involved in the program, and approved by the Institutional Review Board (IRB), may have access to medical records as required by their research protocol. Authorization from the patient must be obtained to release records for medical research.

### ***Attorneys, Insurance Companies, Third Party Payment***

Information from the record may be released upon receipt of proper authorization from the patient, a parent or guardian, the executor of the estate of a deceased patient, persons holding a power of attorney for a patient, third party payers, and insurance companies.

### ***Law Enforcement Agencies***

Members of the FBI or police department who request medical information in the absence of proper documentation must be referred to the physicians of this practice. A legal warrant for search of a patient's records is required for the release of the file. Subpoenas for medical records must be reviewed by a provider of this practice.

### ***Mental Health Record***

Records for mentally ill or mentally handicapped persons must have a medical release authorization form from the legal guardian. These requests also require the approval of the health provider prior to release. The request form and the approval of the physician must be documented in the medical record.

### ***Marketing***

It is the policy of this practice that patient contact information is never released for marketing purposes. Written permission must be given by the patient to release their contact information for healthcare supplies and services.

## **Accounting of Disclosures of a Patient's Protected Health Information**

One of the rights granted to patients under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the right of the patient to request and receive an accounting of all disclosures made of the patient's PHI.

### ***Procedure***

Individuals who release a patient's PHI will document those disclosures in the patient's record. Documentation of releases should be maintained for easy review. This applies to all releases:

- Made after April 14, 2003;
- Made to carry out treatment, payment, or healthcare operations;
- Made to the patient;
- Made to all persons involved in the patient's care;
- To federal officials for national security or intelligence purposes;
- To a correctional institution or law enforcement official that has custody of a patient;
- Releases for payment.

- For purposes of public health activities;
- For judicial and administrative proceedings;
- To coroners, medical examiners, and funeral directors;
- For organ, eye, or tissue donation purposes;
- For research purposes;
- For workers' compensation.

The information that must be documented for each disclosure is:

- The date of the disclosure;
- The name of the person or organization who received the PHI and the address and contact information;
- A brief description of the PHI disclosed;
- A brief statement of the purpose of the release.

***Required patient action***

Patient requests for an Accounting of Disclosures must be submitted in writing to the medical records department of this practice.

When a request is received, the records department will respond within 5 business days with the accounting of records release. A copy of the account will be copied to the patient's record.

**Disclosures of a Patient's Protected Health Information to Individuals Involved in the Patient's Care or for Purposes of Notification**

This practice may release care information to a family member, friend, or other individuals the patient identifies as being involved in the patient's care. This information will be limited to health-related signs and symptoms and to information that helps the patient deal with his/her illness or treatment.

This practice may also disclose a limited amount of the patient's PHI in order to locate the patient or notify a patient's family member or friend. The amount of information to be released must be authorized by the physician.

***When the patient is physically present or otherwise available.***

An individual who is physically present with the patient will be assumed to be an individual who is directly involved in the patient's care unless the patient specifically states otherwise.

Documentation such as pre-printed discharge instructions, patient education forms, and other materials, may be provided to the patient's family member or friend or other person directly involved in the patient's care.

Copies of a patient's PHI may only be released to a patient's family member, friend of the patient, or someone directly involved in the patient's care if the individual presents a signed authorization from the patient.

When the patient is unable to communicate, it will be assumed that the person with the patient is directly involved in their care. Verbal consent to release records must be obtained in the patient's physical presence for all patients able to communicate.

***Releasing a patient's PHI for purposes of locating the patient or locating or notifying a patient's family member or friend of the patient.***

In cases of medical emergency, it will be up to the physician in charge of the patient's care the amount of information that will be released for the purpose of locating the patient.

## **Communicating Protected Health Information via Electronic Mail (E-mail)**

Encrypted information can only be transmitted by employees trained and authorized to use the electronic "keys." Employees not trained in the procedures for encrypted information may not have access to the keys. Unauthorized use of keys will result in immediate termination.

Premier Primary Care will permit email of unencrypted Protected Health Information (PHI) under limited circumstances where the appropriate safeguards are applied.

### ***Procedure***

#### ***Communicating PHI via E-mail Internally***

As a general rule, unencrypted email should not be used to communicate PHI. However, email of PHI will be permitted if certain safeguards are implemented.

The following safeguards must be followed when communicating PHI in, or attached to an email message:

- E-mail communications containing PHI will be transmitted only on Premier Primary Care's email system.
- PHI will never be transmitted in the subject line of the e-mail message.
- The fact that the message or an attachment to the message contains PHI will be reflected in the subject line of the e-mail message using this tag line "Confidential information."
- The email message will include the following confidentiality notice:
- "This electronic message is intended to be used only by the named recipient, and may contain information that is confidential or privileged. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of the contents of this message is strictly prohibited. If you have received this message in error or are not the named recipient, please notify us immediately by contacting the sender at the electronic mail address noted above, and delete and destroy all copies of this message. Thank you."
- This confidentiality notice can be added to the signature block of your e-mail signature if you currently use an automated signature.
- Unencrypted PHI that is specially protected (i.e., HIV/AIDS information, substance abuse treatment information, and mental health information) will not be communicated via e-mail.
- If a document that contains PHI is attached to the message, verify that the proper document has been attached before transmitting the e-mail message.
- Before transmitting the e-mail message, double-check the message and any attachments to verify that no unintended information is included.
- If you communicate PHI via e-mail, you must comply with all other Practice policies and procedures.

### *Communicating PHI with Patients*

Patients have the right to request communication via email. If a patient requests e-mail communications containing their PHI, the employee receiving the request must obtain a completed *Request for Email Communications* form from the patient AND must provide the patient with information about the risks of email transmission prior processing the patient's request.

The Practice reserves the right to deny a patient's request to communicate with him or her via e-mail.

If the patient's initial request to communicate via email is granted, the patient will be required to complete the following prior to engaging in provider/patient emails:

- Send and respond to a test email with answers to a question specific to that patient (i.e., the patient's date of birth, father's name, mother's name, etc.) to verify the patient's email address and identity.
- Acknowledge receipt of the *Important Information about Provider/Patient Email* form confirming the patient's understanding of the risks of engaging in email communications with his/her providers.

No specially protected PHI (i.e., HIV/AIDS information, substance abuse treatment information, and mental health information) will be communicated via email even if the patient's request for email communications is granted.

All completed *Request for Email Communications* forms will be maintained in the patient's record. Approved requests are valid as long as a hard copy of the form is maintained.

An approved Request will be effective for only the health care provider identified on the Request. The patient must complete a separate Request for each health care provider with whom he/she wants to communicate via email, and must revoke each Request to discontinue email communications.

### *Ownership of Electronic Mail*

The Practice email systems belong to the Practice. The Practice reserves the right to override individual passwords and access the email system at any time for valid business purposes such as system maintenance and repair and security investigations.

### *Retention of Email*

The Practice regularly archives email for the purposes of record recovery and regulatory compliance.

## **Fax Policy**

This practice will adhere to the following procedures to protect the confidentiality of Protected Health Information (PHI) when transmitting or receiving it by facsimile (fax):

### *Sending Faxes*

Employees will transmit PHI by fax only when the transmission is time-sensitive. Employees will take reasonable steps to ensure that a fax transmission is sent to and received by the intended recipient. Employees will confirm with the intended recipient that the receiving fax machine is located in a secure area.

- Fax machines will be pre-programmed with numbers of other local healthcare providers to avoid mistakes.
- Numbers entered manually must be verified before confidential information is sent.

- The name, business affiliation, telephone number and fax number of the intended recipient as well as the number of pages contained in the transmission will also appear on the cover sheet.
- The fax confirmation log will be checked immediately after sending a fax.
- If an employee becomes aware that a fax was sent to the wrong fax number, the employee will immediately attempt to contact the recipient and request that the faxed documents be destroyed.
- Fax confirmation sheets will be attached to and maintained with all faxed materials.
- Highly sensitive PHI (such as HIV/AIDS results or status or substance abuse and mental health treatment records) should never be sent by fax.

#### *Receiving Faxes*

Employees who are intended recipients of faxes that contain PHI will take the following steps to ensure the intended recipient only views the fax

- Fax machines that receive PHI will be kept in secure areas.
- Fax machines will be checked on a regular basis by authorized staff to minimize the amount of time incoming faxes are left on the machines.
- Only the addressee should read faxes.
- Should the Practice's FAX number change for any reason, the business manager (or assigned staff member) will send notify all of the healthcare providers from whom this practice typically receives faxes of the change.

## **Rights of Minors to Keep Certain Categories of Protected Health Information Confidential**

HIPAA provides individuals with certain rights related to their PHI, including the right to request their PHI be kept confidential. Although minors do not generally have the authority to exercise rights on their own behalf, state law and HIPAA provide minors with the authority to exercise control over certain categories of their own PHI.

A minor's health care provider must maintain the confidentiality of a minor's medical records under the following circumstances:

#### *Procedures*

A minor who is over the age of twelve (12) may seek and receive the following types of health care services without parental consent.

- HIV/AIDS testing and treatment;
- Testing and treatment for venereal and sexually transmitted diseases;
- Pregnancy and pre-natal care;
- Chemical dependency services; and
- Mental health outpatient services.

A minor's personal representative does not have the right to the minor's PHI if the minor alone consented to the treatment, unless the minor authorizes the release.

### ***Abuse***

If the health care provider reasonably believes the minor has been or is subject to domestic violence, abuse, and/or neglect by the minor's parent or guardian, keeping the minor's PHI related to the abuse confidential is in the best interests of the minor. The policy of this practice is to notify the physician of any requests for release of information in cases of suspected abuse.

When the minor's parent or guardian requests information and it is denied the following procedure applies:

- Notify the requester that he/she may request a review of the denial by the physician in charge of the minor's care.
- An explanation of HIPAA policy will be sent within 5 business days.

Any questions about whether a minor's PHI is confidential should be brought to the attention of the minor's physician.

### ***Requests for PHI from the minor's school***

If the minor's school requests medical records,

- The minor's written authorization for the release must be documented in the patient file or
- Written authorization from the parent or guardian must be documented in the patient file.
- In the case of public health, the patient's physician should be consulted prior to the release of any information.

Vaccination records and other medical information may be released upon receipt of proper authorization from the patient or patient's legal guardian. If the request is for the information to be sent electronically either by fax or email, the authorization form must contain the fax number or email address. Only the specific information requested will only be sent.

## **Distribution of the Notice of Privacy Practices**

HIPAA mandates the distribution of a Notice of Privacy Practices to all patients. This notice shall include:

- The procedure for releasing information from this practice.
- The patient's rights and responsibilities regarding his/her PHI;
- This practices responsibility regarding the patient's PHI.

All patient's will be given a HIPAA notice and asked to sign an acknowledgment of receipt. This will be kept in the patient's file and updated annually.

If the patient refuses to acknowledge receipt of the HIPAA notice, document the patient's refusal on the acknowledgment form along with any efforts that were made to obtain the patient's signature. Place this in the patient's file.

## **Ownership and Control of Original Records Containing Protected Health Information**

When a patient supplies information and records, these documents will be copied and returned to the patient within 3 business days.

***Removal of a patient's records***

Records are not removed from a patient's file except by court order.

***Disposition of original records upon departure of a health care provider***

Patient records are not destroyed. When a patient leaves the practice, records are kept for five years. The patient is offered a copy of his records at his last appointment. These copies will be mailed within 10 business days to the address supplied by the patient.

**Patient Complaints about Uses and Disclosures of their Protected Health Information**

Any complaints about the release of medical records by the patient should be brought to the attention of the physician in charge of his/her care.

**Exercising Patient Rights Related to Protected Health Information**

Patients are granted numerous rights regarding their protected health information (PHI) by HIPAA:

- The right to inspect their PHI and to obtain a copy of it;
- The right to request an amendment to their PHI;
- The right to an Accounting of Disclosures.
- The right to request restrictions on the uses and disclosures of their PHI.
- The right to request that all communication regarding their medical records be sent to a special location or phone number.
- The right to receive a paper copy of this practice's HIPAA policy.

The patient can exercise any of these rights by submitting a written request to the medical records department.

**Confidentiality of Psychotherapy and Personal Notes**

Psychotherapy and personal notes are considered the property of the health care provider who created them, and will not be released or disclosed to patients.

**Disclosures of Protected Health Information Required by Law**

All PHI at this practice is confidential, and would not normally be released. There are circumstances where we are required by law to report medical information to the proper authorities for the greater good of public health.

The list of agencies and authorities and the types of PHI that must be reported follows:

<i>Agency/Authority Receiving</i>	<i>Subject/Category of Required Report</i>
City, County, or District Health Official	Suspected or confirmed cases of communicable diseases
Local Health Official	Exposure to animal suspected of having rabies

Local Health Official	Patients infected with tuberculosis who vacate their residence by death or removal from the premises
Local Health Official	Pregnant women who test positive for Hepatitis B
Local Health Official	Syphilis tests on pregnant women
National Practitioner Data Bank	Specified information regarding malpractice payments and adverse actions
City/County Department of Health	All immunizations administered to any child under the age of seven
City Department of Health	Cases, carriers, and persons who at their time of death were affected by any of the communicable diseases
	Deaths - caused by natural causes
	HIV, HIV-related illness, and AIDS occurring within New York City
	Deaths - not a result of natural causes
	Tuberculosis
	Births
	Syndromic surveillance information (real-time reports of the chief complaint, home zip code, sex, age, and unique identifier of patients seen in the Emergency Room within the past 24 hours)
State Board of Medical Examiners	Specified information regarding malpractice payments and adverse actions
State Central Register of Child Abuse and Maltreatment	Suspected child abuse or maltreatment; failure to immunize infants for Hepatitis B if the mother is Hepatitis B positive
State Department of Health	Alzheimer's disease upon diagnosis or confirmation of presence of illness
	Cardiac reporting
	Cases of communicable diseases diagnosed after death
	Habitual narcotics users
	Hepatitis B test results for all women with newborn children
	HIV, HIV-related illness, and AIDS occurring outside of New York City
	Increased incidence of nosocomial infections or nosocomially acquired communicable disease
	Radioactive cadavers
	Sexually transmissible diseases (STDs)

	Statewide Planning and Research Cooperative System - data specified
	Patient death due to an act of omission or commission by a member of the ambulance service
State Bureau of Environmental Protection	Persons who have clinical evidence of occupational lung disease
State Department of Health's Wadsworth Center Laboratories	Blood sample from every newborn to be tested for certain diseases
State Office of Fire Prevention and Control	Burn injuries - Second or third degree burns to 5% or more of the body.
State Office of Mental Health	Aggregate data relating to incident reporting
State Office of Mental Retardation and Developmental Disabilities	Aggregate data relating to incident reporting
Occupational Safety and Health Administration (OSHA) - Area Office	Death of an employee or multiple employee injuries
Police	Violent injury - Bullet wound, gunshot wound, powder burn, other injury caused by a gun or firearm. All injuries that are likely to or do result in death and appear to be caused by a knife, ice pick, etc.
Regional Health Director or Associate Commissioner for New York State	Nosocomial infections
US Department of Health & Human Services - CMS	Deaths - caused by restraint or seclusion
US Department of Labor	Death of an employee or multiple employee injuries

The person providing PHI in response to a mandatory reporting requirement is responsible for documenting the name, title, and contact information of the individual to whom the PHI was provided as well as the agency name and address, the date, and a brief summary of the information provided.

***Responding to law enforcement inquiries***

It is the policy of this practice to assist law enforcement in every way possible. However, we have a responsibility to protect our patient's privacy. Before information can be released we must have:

- A written release from the patient; or
- A subpoena, court order or warrant.

Any requests for information from law enforcement officers should be referred to the patient's physician.

*Responding to Inquiries from National Security, Intelligence, and Protective Services Officials.*

Any requests for information from a patient's medical record for purposes of national security must be referred to the patient's physician.

**Releasing Protected Health Information to Prevent a Serious Threat to Health or Safety**

Any law enforcement officer requesting patient information for purposes of public safety should be immediately referred to a physician.

**Unauthorized Uses and Disclosures of a Patient's Protected Health Information**

Disciplinary action may be taken against any employee who violates any HIPAA policy or procedure. It is the responsibility of the employee to acquaint themselves with the policies and procedures of this practice.

Disciplinary actions may include but are not limited to:

- A letter to the employee's personnel file;
- Administrative leave without pay;
- Attendance and successful completion of additional training;
- Reimbursement of expenses incurred by this practice;
- Immediate termination of employment;
- Referral for criminal investigation if the violation was intentional.

*Violations of state or federal confidentiality laws and regulations*

Disciplinary action will also be taken against employees violating related state or federal confidentiality laws and regulations.

**Disclosures of Protected Health Information Over The Telephone**

It is the policy of this practice not to release information over the phone until a fax of a signed authorization is received from the requesting party. The exception is in the case of a medical emergency. The request for emergency information should be handled by a nurse and document in the patient file with the following information: Date, name and contact information of the requesting party, the name of the facility of care provider and the specific information released.

**Releasing Information for Purposes Of Treatment, Payment and Health Care**

The policy of this practice is to release information only with signed authorization from the patient.

- Authorization to release information for insurance and payment processing must be obtained on the first visit prior to being seen by a provider from this practice.
- This authorization must be updated annually.
- Medical record information may be used to provide treatment services.

- Medical information can be shared with other physicians with the patient's written authorization.
- The information may be used to bill and collect for the treatment and services provided to the patient.
- Information may be release to the patient's health plan to obtain prior approval for treatment and/or to determine whether the patient's plan will cover the treatment.

### **Confidential Information Used by Subcontractors or Vendors**

Should Premier Primary Care decide to subcontract billing services, or higher a systems designer or other vendor to help securing confidential patient information, such vendors and subcontractors will be bound by the policies and procedures of the Practice. Prior to commencing work, a statement of HIPAA compliance will be secured by the business manager.