

# Notice of Privacy Practices

This office will provide a Notice of Privacy Practices (NPP) as required by 164.520 no later than the first date of service delivery including service delivered electronically. This notice will outline how protected health information will be used or disclosed and also detail the patient's rights under the regulations. The provision of the NPP to the patient will be documented on the Acknowledgement of the Receipt form.

The following steps will be taken to ensure the patients receive and have access to a copy of this facility's NPP as required by law.

- A NPP will be given to every new patient no later than the first date of service delivery.
- When care is first delivered onsite the patient will be given a copy of the NPP and the Acknowledgement of Receipt form.
  - If the patient refuses to sign the Acknowledgement of Receipt form, a staff member will document on the form that the NPP was provided to the patient.
  - When care is provided in an electronic format or via telephone services, the patient will be mailed a hard copy of the NPP along with the Acknowledgement of Receipt form.
  - Or if the patient consents, a copy of both forms will be emailed at the time the patient requests services. The delivery of the NPP will be documented in the patient record. If this office becomes aware of the failure of the email transmission, a hard copy of the NPP will be mailed to the individual.
- The patient will be asked to sign and return the Acknowledgement of Receipt form. If the form has not been returned, at the first on-site visit the patient will be asked to sign the Acknowledgement of Receipt form.
- In the event of an emergency situation, as soon as possible, the NPP will be given to the patient and the signature of receipt obtained. The emergency conditions will be documented in the patient record.
- The NPP will be posted in a prominent location in the practice.
- Any patient requesting a hard copy of the notice will be provided a copy.
- On or after the effective date, in the NPP is revised, the revised version will be available upon request for current patients. A new Acknowledgement of Receipt for will not be required.
- Once revisions are made to the NPP, a copy if a NPP will be archived for a period of not less than six (6) years from the last effective date.

- This office has a website.
  - The NPP is posted on the website and is available electronically.

## Safeguarding Protected Health Information

This office will implement appropriate safeguards to protect patient health information whether in written, oral, or electronic format to reduce the likelihood of an inappropriate or unauthorized use or disclosure.

### *Verbal Communication*

- Workers must be aware of their surroundings when conversations occur which involve protected health information.
- Discuss issues in a secure location (patient room or office), especially in the case of conversations regarding sensitive issues such as discussion of communicable diseases or financial issues.
- Discuss patient information only with workers involved in the care of the patient.
- Dictation and telephone conversations should occur away from public areas whenever possible.
- When leaving telephone voice messages or appointment reminders, always ensure only to leave the minimum necessary information. For instance, “this is Dr. Smith’s office calling” as opposed to, “this is Sally from West End Oncology calling.”

### *Faxing of Information*

- Pre-program frequently used numbers for faxing.
- Utilize a cover sheet with a confidentiality statement for any fax containing protected health information. Suggested wording is located in the Supplemental Section of the HIPAA Manual.
- Only fax the minimum necessary information needed to meet the needs of the requesting party.
- Do not fax information for other than treatment, payment, or healthcare operations without an approved authorization by the patient.
- Whenever possible, confirm receipt of the fax. Attach confirmation information to the fax to be included in the patient record.
- Fax machines will be located in secure areas of the office which are not easily accessed by patients and visitors. Faxes should be removed from the machine as quickly as possible and filed appropriately or placed in a secure shred bin.

### *Training*

- All workers, including volunteers and students, will be trained in the HIPAA Privacy and Security Rules. The training will occur within a reasonable period of time when a new member joins the workforce and annually thereafter.
- This training will include a review of the pertinent regulations, definition of breach, and safeguards to protect patient information.
- Documentation of training will be kept for a period of no less than six (6) years by the Privacy officer or office manager.

### *Patients and Visitors*

- Patients will be accompanied to the patient care area.
- Visitors, which include manufacturer representatives and repair personnel will only be allowed access to approved areas of this office.
- Movement within the office will be monitored to ensure inappropriate access to protected health information is not obtained.

### *Paper Copy of Records (Medical and Financial)*

- Paper copies of records will be secured in some manner when left unattended.
  - Placed faced down when on counters/desk or when placed outside an exam room door.
  - Medical records area of the office is locked at all times.
  - Medical records area of the office is not locked, but only authorized personnel are allowed to enter.
  - Workers are not allowed to take health records out of the physical location of this practice unless transporting to a satellite office. Security measures will be taken when records are transported.

### *Disposal of Protected Health Information*

- Any media containing protected health information should only be discarded in the appropriately identified containers.
- Paper copies of information which are waiting disposal will be placed in a secure storage container/area before shredding occurs.
- Electronic media will be destroyed according to procedures included in the Security Plan.

### *Computers*

- Computers will be positioned so that protected health information cannot be viewed by unauthorized personnel.
- Workers will log off or lock their computers when left unattended.

### *Social Media*

- Workers are not permitted to discuss patient information on any personal social media account, including just the patient's name.
- Workers should refrain from accessing person social media accounts on network computers.

### *Emailing of Personal Health Information*

- Email communication which includes health information, will occur in a secure manner.
- This office does not have a secure means of emailing patient information outside of this office.
  - Workers in this practice will not initiate an email containing protected health information.
  - Limited information will be sent via unsecured email. Additional protections include:

- 
- If a patient requests this office to send protected health information, we will alert the patient to the risk of sending the information in an unsecured manner.
    - We honor this request once the patient has signed an authorization form.
    - We will not send unsecured email.

# Acknowledgement of Receipt of Notice of Privacy Practices

Patient Name: \_\_\_\_\_

Address: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

I, \_\_\_\_\_, have received a copy of this office's Notice of Privacy Practices.

Please Print Name: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

TO BE COMPLETED BY PATIENT

## FOR OFFICE USE ONLY

We were unable to obtain a written acknowledgement of receipt of the Notice of Privacy Practices because:

- An emergency existed and a signature was not possible at the time.
- The individual refused to sign.
- A copy was mailed with a request for a signature by return mail.
- Unable to communicate with the patient for the following reasons:

\_\_\_\_\_

\_\_\_\_\_

Other: \_\_\_\_\_

Prepared By: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

TO BE COMPLETED BY PRACTICE