**FAX, PHOTOCOPY, TEXT, AND EMAIL PROCEDURES**

To adequately meet HIPAA requirements, this Practice adheres to special faxing, photocopying, texting, and emailing procedures in order to protect patient information. There are certain risks involved when sending or receiving PHI by any of these methods, the result of which is that the PHI may be received by someone other than the intended recipient, or that the Practice may receive PHI that was not intended to be sent to the Practice. To minimize the risks, all staff members are required to understand and adhere to the following procedures.

**Faxing PHI**

To minimize the risks associated with faxing PHI, the following procedures must be followed:

* The PHI will not be faxed unless the Practice determines that it is absolutely necessary that the PHI is transmitted and received more quickly than if sent by first class mail.
* Prepare the appropriate fax cover sheet. Use the *Release of Information via Fax Transmission* form.
* If you are not certain that the fax number is correct, call the recipient first to confirm that the number is accurate.
* Once the fax has been transmitted, check the fax number on the machine acknowledgment to be certain that it corresponds to the number on the fax cover sheet, and then attach the acknowledgment to the copy of the fax cover sheet.
* If the fax is urgent or the information sent is extremely sensitive, telephone the recipient of the fax to make certain that the fax was received.
* Place the documentation in the patient’s file.

**Receiving Faxes**

If a fax is received, the following procedures must be followed:

* If the fax is not intended to be received by the Practice, immediately call the sender of the fax and inform them that the fax was received. Tell that person that the fax will be destroyed.
* Faxes that are received should be delivered to the intended recipient as soon as possible. If an employee notices that a fax has been received, the employee will check the cover sheet on the fax and immediately notify the person who is the intended recipient of the fax.
* Do not leave faxes sitting on the machine where they could be picked up by unauthorized persons.

**Photocopying PHI**

It is often necessary to photocopy a patient’s PHI. In order to make certain that the PHI that is being photocopied will be protected from an improper disclosure, the following procedures must be followed:

* The person making the copies will first count the number of pages to be copied.
* Once the copies are completed, count the original and the copies to make certain that they are identical in number.
* Before leaving the copy machine, check the machine to make certain that none of the originals or copies have been left behind.

**Text Messaging**

Text messages are electronic communications sent with a mobile device or computer system. Text messages can transmit photos, videos, and written word formats. ALL text messages containing ePHI MUST be sent in a secure, encrypted, and approved format. <IF YOUR PRACTICE HAS AN ENCRYPTED TEXT MESSAGING SERVICE, INCLUDE THAT INFORMATION HERE> Texting (short message service (SMS)) allows for more timely communication between the Practice and our patients. However, there are certain risks involved when texting, the result of which is that confidential information may be received by someone other than the intended recipient. To minimize the risks associated with texting, the following procedures must be followed:

* **Consent**: Do not text any PHI to the patient or members of the public without their written consent using the *Authorization for Text Messaging* form.
* **Security**:
  + Password protect the phone or device used for sending the text messages.
  + Confirm that the cell phone number of the patient is recorded correctly.
  + Mobile devices used to send messages MUST be secure at all times, including at home and work.
  + Never disable the password protection feature.
  + Mobile devices must be configured to lock automatically after a period of inactivity (not to exceed 5 minutes).
  + Mobile devices used to text ePHI must be properly sanitized upon retirement of the device. If an employee uses a personal device, they must securely wipe (sanitize) the device before returning it to their mobile device provider.
* **Incorrect recipient**: Report all text messages that are sent to the wrong intended individual to the HIPAA Security Officer.
* **Message content**: SMS text messages must not contain PHI. Inform patients to never send PHI when texting the Practice. Do not store first and last names in the address book used for sending text messages. Store first name and last initial only. Never use first and last name in a text message.
* **Storing and deleting messages**: Delete text messages after communication is completed and necessary information is documented appropriately (see “Documentation” below).
* **Patient generated messages that include PHI**: Do not reply to the original text; instead, send a new message that asks the patient to call you. For example, “I am unable to provide confidential information in a text message. Please call xxx-xxx-xxxx.”

Note: Immediately report received text messages that contain any ePHI to the HIPAA Security Officer.

* **Information included in messages**:
  + The following MAY be included in a text message: your name, your phone number, a statement that identifies you, <IF YOUR PRACTICE NAME IDENTIFIES SENSITIVE HEALTH INFORMATION (E.G., HIV CENTER, MENTAL HEALTH CLINIC, ETC.) REMOVE THE STATEMENT IDENTIFYING YOUR PRACTICE> request for the patient to call you, patient, appointment time and/or location, or missed appointment reminder.
  + Do NOT include any of the following: PHI, information that identifies you as a health care provider or specialist, client referral information, patient orders.
  + If you are unsure about how to respond appropriately, please contact <INSERT THE NAME OF THE MANAGER TO CONTACT>.
* **Documentation**: Be sure to include documentation in the patient record that communication has occurred. It is critical to identify that communication has taken place. For example, “Text message sent to inform patient of appointment reminder on xxx.” Documentation should include the date and time of the communication. Be sure to also document text messages initiated by the patient, as well as your response.
* **Best practice reminders**:
  + Be aware of tone. Be professional at all times and do not use shorthand or abbreviations.
  + Text messages should be short and concise (less than 160 characters), otherwise it will likely be split into two separate messages.
  + Review texts before sending to ensure accuracy. Beware of autocorrect issues.
  + Rapid responses are expected. Be sure the patient understands the Practice’s policy of <INSERT YOUR POLICY REGARDING WHETHER YOU WILL CONTINUE A DIALOG AND HOW SOON THEY SHOULD EXPECT A REPLY>.
  + Be aware that some people may not have text messaging as part of their cell service plan and additional charges could apply. Be sure they understand that they could be charged for each text message.
  + Personal text messaging with patients is strictly prohibited.

**Sending Emails**

All emails must include the appropriate disclaimers and warnings about PHI and should be sent with proper encryption methodologies. However, the patient may elect, at their own assumption of risk, to have their PHI submitted via unsecured email.

When sending any emails containing PHI or other business information, our office uses <NAME THE ENCRYPTION METHOD USED> to protect the information being sent. Also, we use the following approved disclaimer and warning on every email:

*“This email, including attachments, is CONFIDENTIAL and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error, please notify the sender immediately by email and delete all of this email from your system.*

*“This message contains confidential information and is intended only for the individual named. If you are not the intended recipient, you are notified that disclosing, copying, distributing, or taking any action in reliance on the contents of this information is strictly prohibited.”*

**Verification**

Additionally, we will use reasonable measures to verify the individual who is requesting the PHI is who they claim to be and that we have the correct contact information (e.g., email address, cell phone number) to send the information. We will:

* Obtain written authorization that the patient understands the unsecured nature and inherent risks of having PHI texted, emailed, or faxed to them.
* Explain the unsecured nature of using emails so that the patient understands and accepts the responsibility of receiving their PHI this way.
* <INSERT THE PRACTICE’S METHODOLOGY OF VERIFICATION, (E.G., CHECK THEIR DRIVER’S LICENSE OR OTHER FORM OF ID, SENDING A VERIFICATION TEXT, ETC.)>
* Double-check their mobile number or email address with them to verify that we have the correct information before we send the message with attached PHI.