



PEDIATRIC PARTNERS, P.A.

PEDIATRIC PARTNERS POLICY ON IDENTIFY THEFT

It is the policy of Pediatric Partners, P.A. (the “**Practice**”) to protect confidential patient information. The Practice has adopted a program to detect, prevent and mitigate identity theft in connection with any covered patient account.

On April 20, 2009, the Board of Directors of Pediatric Partners, P.A. approved and adopted its initial Identity Theft Prevention Program (“**Program**”). The Program was developed in order to comply with the Federal Trade Commission’s Identity Theft Prevention Red Flag Rule (16 CFR § 681.2). The Program has been created in consultation with the practice’s human resources director, office manager, attorney and managing partner, after conducting an assessment of risk of identity theft (“**Identity Theft**”) associated with certain Covered Accounts.

A “**Covered Account**” means (i) any account that the Practice offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions, including one or more deferred payments; and (ii) any other account the Practice identifies as having a reasonably foreseeable risk to patients or to the safety and soundness of the Practice from Identity Theft. As of April 20, 2009, the Practice has identified the following types of accounts as Covered Accounts:

1. Patient billing when payment is not made at the time services are rendered (whether the future payment is to be made by the patient or by the patient’s insurance plan)
2. Patient payment plans established between the Practice and the patient’s parents, guardians, legal representatives or any third party, as the case may be.

“**Identity Theft**” means fraud committed using the identifying information of another person.

“**Red Flag**” means a pattern, practice or specific activity that indicates the possible existence of Identity Theft.



PEDIATRIC PARTNERS, P.A.

RED FLAGS IDENTITY THEFT PREVENTION PROGRAM

Pediatric Partners, P.A. will comply with The Federal Trade Commission (FTC) “Red Flag Rule” to identify any practice or specific activity that indicates the possible existence of identity theft. The following procedures (“the Program”) have been established to protect individual identity:

- I. Identity of Relevant Red Flags**
 - A. Presentation of suspicious documents
 - B. Presentation of suspicious personal identifying information
 - C. Unusual or suspicious activity related to a covered account
 - D. Notice from authorities or other persons regarding possible identity theft in connection with a covered account
- II. Detection of Red Flags**
 - A. Patient cannot produce an insurance card or other physical documentation of insurance
 - B. Documents provided for identification appear to have been forged or altered
 - C. Personal identifying information provided is not consistent with other personal identifying information provided by the patient (such as inconsistent signatures, different photos, etc.)
 - D. The SSN provided appears to have been submitted by another patient
 - E. Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient
 - F. Inquiry from an individual based on receipt of an invoice or document for another individual, or for healthcare services not received
 - G. Mail sent to the patient is returned repeatedly as undeliverable
 - H. Frequent change of address
 - I. Invalid phone numbers
- III. Prevention and Mitigation of Identity Theft**
 - A. Require parents, grandparents, guardians or any other person who bring children to our office for care to provide verification of identity by showing a current driver’s license
 - B. Monitor covered accounts for evidence of identity theft
 - C. Investigate patient complaints and review records to identify any inaccurate information and re-verify identifying information with patient
 - D. Investigate complaints and interview patients as appropriate and re-verify identifying information with patient
 - E. Notify law enforcement as appropriate
 - F. Require that service providers who perform activities in connection with Covered Accounts have policies and procedures in place designed to detect, prevent and mitigate the risk of Identity Theft with regard to Covered Accounts
- IV. Updating and Reviewing of the Practice’s Identity Theft Program**
 - A. Prepare an annual report on the first of May of each year which would include any identified theft incidents and the responses made
 - B. Review of the effectiveness of the program and procedures, including any recommended changes
 - C. Continue to monitor information on new identity theft threats
 - D. Continue to verify identifying documents and updating of covered patient accounts
- V. Training for Pediatric Partners’ Personnel**
 - A. Provide identity theft prevention training for all practice personnel
 - B. Training to be supervised by the Human Resources Director, Office Manager or Attorney
 - C. New personnel will receive identity theft prevention training as part of their orientation