ADVANCED DENTISTRY
OF PLYMOUTH MEETING
RESTORATIVE • IMPLANT • COSMETIC

832 Germantown Pike, Suite 1
Plymouth Meeting, PA 19462
Office 610.277.0996, Fax 610.275.5075
info@plymouthmeetingdentistry.com
www.plymouthmeetingdentistry.com

Identity Theft Prevention Policy Plymouth Meeting Dental

This Identity Theft Prevention Program ("Program") is designed to comply with the Federal Trade Commission's Identity Theft Red Flags Rule (16 CFR § 681.2). The purpose of this Program is to detect, prevent and mitigate identity theft in connection with PMD's Covered Accounts (defined below).

I. Definitions

A. "Covered Account" means (i) any account Plymouth Meeting Dental (here in known as PMD) 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 PMD identifies as having a reasonably foreseeable risk to patients or to the safety and soundness of PMD from Identity Theft. As of the date of approval of this Program, PMD has identified the following Covered Accounts:

1) patient billing accounts;
2) patient payment plans; and
3) third-party financing.

B. "Identity Theft" means fraud committed using the identifying information of another person.

C. "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

II. Identifying and Detecting Red Flags

PVDG's Identity Theft Mitigation and Prevention Procedures, attached as Appendix A, contain Red Flags identified by PVDG as relevant to the size and complexity of PVDG and the nature and scope of its activities as of the date of this Program. In order to facilitate detection of the Red Flags identified in Appendix A, PVDG verifies the identity of patients seeking to open new accounts and authenticates the identity of patients with respect to actions involving existing accounts.

Verification and authentication procedures include requiring sufficient current identifying information in order to establish an individual's identity (e.g., full name, date of birth, phone number, physical address, social security number, government issued identification card, insurance card, etc.). These procedures should be read in conjunction with PVDG's HIPAA policies and procedures, as contained in PVDG's HIPAA Compliance Manual.

III. Preventing and Mitigating Identity Theft

Each Red Flag identified in Appendix A is paired with a suggested response designed to prevent and mitigate identity theft. If a fraudulent activity involves personal health information ("PHI") covered under HIPAA, PVDG's HIPAA policies and procedures will also be followed in response to the activity.

IV. Program Administration and Oversight

PVDG is responsible for developing, implementing, administering and updating the Program. PVDG is responsible for training staff identified as responsible for, or having a role in implementing, the Program.

PVDG will, in all contracts executed from the date of this Program forward, require service providers performing activities in connection with Covered Accounts to have policies and procedures in place designed to comply with the Federal Trade Commission's Identity Theft Red Flags Rule (16 CFR § 681.2).

Appendix A Identity Theft Mitigation and Prevention Procedures

IDENTITY THEFT RED FLAG	PREVENTION/ MITIGATION PROCEDURE	RESOLUTION OF RED FLAG
Documents provided for identification appear suspicious (i.e. appear to have been altered, forged, reassembled or otherwise tampered with).	Stop any billing processes. Require applicant to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy.
Personal identifying information provided is inconsistent with other information on file or is the same or substantially similar to that used by another patient or patients. Such information may be provided by the patient or otherwise available through internal or external sources. (i.e. physical appearance does not match physical description, lack of correlation between the Social Security Number ("SSN") range and date of birth, address given does not match address on file, etc.)	Stop any billing processes. Require applicant to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy.
Records showing treatment that is inconsistent with a physical examination or with a medical history as reported by the patient.	Investigate complaint, interview individuals as appropriate, review previous files for potential inaccurate records. Items to consider include: blood type, age, race, and other physical descriptions that may be evidence of medical identity theft.	Depending on the inconsistency and review of file, either delay/do not open a new covered account, or terminate services. Notify PVDG as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.

IDENTITY THEFT RED FLAG	PREVENTION/ MITIGATION PROCEDURE	RESOLUTION OF RED FLAG
Complaint/inquiry from an individual based on receipt of: - a bill for another individual - a bill for a product or service that the patient denies receiving - a bill from a health care provider that the patient never patronized - a notice of insurance benefits (or Explanation of Benefits) for health services never received.	Investigate complaint, interview individuals as appropriate.	Terminate treatment/credit until identity has been accurately resolved; refrain from attempting to collect on the account until identity has been resolved. Notify PVDG as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
Complaint or inquiry from a patient regarding credit information, including: health care or health insurer related information added to a credit report or receipt of a collection notice from a bill collector.	Investigate complaint, interview individuals as appropriate.	Terminate treatment/credit until identity has been accurately resolved; refrain from attempting to collect on the account until identity has been resolved. Notify PVDG as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
Insurance-related issues, including, the patient cannot produce an insurance card or other documentation of insurance, or patient or insurance company report that coverage for legitimate dental work is denied because insurance benefits have been depleted or a lifetime cap has been reached.	Stop any billing processes. Require applicant to provide additional satisfactory information to verify identity. Investigate complaint, interview individuals as appropriate.	Additional documentation must be provided to resolve discrepancy and continue billing process. Contact insurance company as necessary. Notify PVDG as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
Mail sent to the patient is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the patient's covered account.	Skip-tracing procedures are used to find the patient's current mailing address.	Patient is found and contact information is updated.