

**PRESERVATION DENTAL  
IDENTITY THEFT  
DETECTION AND RESPONSE  
POLICY AND PROCEDURES**  
*Effective May 1, 2009*

**I. POLICY**

This office has adopted an Identity Theft Detection and Response Policy and Procedures Program (“Program”) pursuant to the Federal Trade Commission’s Red Flag Rules (“Rules”). The purpose of the Program is to assist in detecting, preventing and mitigating instances of possible identity theft in connection with patients in our practice. It does so by (a) requiring us to verify the identity of all new patients, (b) establishing certain “Red Flags” that could indicate possible identity theft, and (c) requiring follow up on any incident which triggers a Red Flag. The Program must be observed by all employees of this practice, including the professional, administrative and clerical staff.

Unless used as an insurance identification number or is otherwise necessary, this practice does not require Social Security numbers from patients.

To the best of our ability, we select service providers who are compliant with the Program pursuant to the Rules.

**II. RED FLAGS THAT MAY INDICATE IDENTITY THEFT:**

- a. An individual falsely claiming to be someone else who is known to the office staff;
- b. An unrecognizable individual with no personal identification or who refuses to provide information about their identity;
- c. Any individual who is unable or unwilling to provide contact information;
- d. Suspicious documents that appear to have been altered or that contain information that does not match the person presenting them;
- e. Altered or cancelled insurance cards;

- f. Attempts to submit by phone a patient's credit card or insurance information as payment for services;
- g. Suspicious requests for a prescription or a refill;
- h. Unexplained discrepancies between the patient's records and the patient's physical appearance and/or condition;
- i. A report by the patient known to the office staff that he or she has been the victim of identity theft in connection with oral health care services provided by the practice;
- j. Any other suspicious activity in relation to patient accounts, including evidence of security breaches (e.g., theft of a computer containing patient information), and unusual activity in relation to such account.

### III. **RESPONDING TO RED FLAGS**

Any employee of this practice who encounters a Red Flag situation or any other activity that may indicate identity theft should report the situation to Denise Jenkins. She will follow up as appropriate and will record the incident and its handling in a Red Flags Log kept in this office.

#### **Possible responses to a Red Flag Situation include the following:**

##### a. **Patient Notification**

The practice may notify the patient if a Red Flag is encountered that involves that patient's identity. Notification may be provided by mail, by telephone, or in-person – as the practice deems appropriate. The notification may include verification that the patient has not been victimized by identity theft in connection with any visits to the practice.

In some instances, additional specific action will be required:

- If notice of an actual identity theft is received, we will immediately cease any collection efforts that are related to the identity theft.

##### b. **Notification of Legal Authorities**

If the practice obtains specific information pertaining to a person committing identity theft, we will provide that information to law enforcement to the

extent permitted under HIPAA and other privacy rules. We may seek advice of legal counsel on the issues involved.

*Of course, if a Red Flag is triggered but we determine that there clearly has been no identity theft, no action will be taken.*

#### **IV. PLAN ADMINISTRATION AND UPDATES**

All employees of this practice will receive a copy of this Policy and will be instructed as to its procedures. We will ask each employee to sign an acknowledgement of receipt and understanding. We will evaluate our Program annually and update it in light of experience. Any questions about this Policy should be addressed to Denise Jenkins.