



FLORIDA SOCIETY OF GENERAL SURGEONS

RED FLAG RULE COMPLIANCE PROGRAM

Prepared by:
Christopher L. Nuland, Esq.
1000 Riverside Avenue, Suite 115
Jacksonville, Florida 32204
(904) 355-1555

Copyright 2009, Christopher L. Nuland. All Rights Reserved, except where otherwise noted.

I. Introduction

The “Red Flag” Rules will become effective on August 1, 2009. Under these rules, “creditors” (which include physician practices that do not collect the full amount of a charge at the time of service) must enact a compliance plan, similar to HIPAA, to protect its patients’ sensitive personal information, which are referred to as “covered accounts.” In fact, if a practice has an effective HIPAA and/or Corporate Compliance Program, the Red Flag Rules can easily be folded into the existing compliance program.

II. Mandated Tasks

- A. The Practice’s Compliance Officer should review the attached Red Flag Rules to determine which are relevant to the Practice;
- B. Identify those employees who are involved in verifying the identity of patients and handling sensitive personal information.
- C. Create a Compliance Plan designed to detect Red Flags in the Practice.
- D. The policy should include a plan for action if and when Red Flags are detected.
- E. The Compliance Plan should be reviewed periodically.
- F. The Board of Directors must officially adopt the new Policy and Procedures; and
- G. The staff must be trained, as necessary, in the policy and procedures.

iii. Policies and Procedures

Policy Number One

Evaluating the Practice

- A. What are the most relevant risk factors that would place a patient’s sensitive financial information at risk?
- B. Has the Practice experienced previous episodes of identity theft? Identify the cause and outcome.
- C. In light of the answers to A and B, what special measures, if any, must the Practice take to protect patients’ sensitive financial information?

Policy Number Two

To the extent allowed by the patient's medical condition, all new patients shall be required to present photographic documentation verifying their identity and address. Change of information shall require documentation.

Policy Number Three

Upon receiving any of the following Red Flags, personnel shall immediately forward the same to the Compliance Officer for evaluation. The Compliance Officer shall determine the action warranted and if changes in the Compliance policies and Procedures are warranted.

- (1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- (2) The presentation of suspicious documents (see Appendix for examples);
- (3) The presentation of suspicious personal identifying information, such as a suspicious address change;
- (4) The unusual use of, or other suspicious activity related to, a covered account; and
- (5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

Policy Number Four

In the event the Compliance Officer believes that a patient's sensitive financial information has been compromised, the Officer may institute any of the following actions:

- (a) Monitoring a covered account for evidence of identity theft;
- (b) Contacting the customer;
- (c) Changing any passwords, security codes, or other security devices that permit access to a covered account;
- (d) Reopening a covered account with a new account number;

- (e) Not opening a new covered account;
- (f) Closing an existing covered account;
- (g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- (h) Notifying law enforcement; or
- (i) Determining that no response is warranted under the particular circumstances.

Policy Number Five

No less than annually, the Compliance Officer shall deliver to the Board of Directors a report detailing the Practice's efforts and compliance with the Red Flag Rules.

The report should address material matters related to the Program and evaluate issues such as: The effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

Policy Number Six

No less frequently than annually, affected staff shall receive in-service training to include:

- (a) The experiences of the Practice with identity theft;
- (b) Changes in methods of identity theft;
- (c) Changes in methods to detect, prevent, and mitigate identity theft;
- (d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and
- (e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances; and
- (f) The types of Red Flags identified by the Code of Federal Regulations (16CFR681 App A).