RED FLAG RULES: What You Need To Know

MICHAEL J. SILESKI, ESQ., MHA
Associate
Karafin & Gruenstein, P.C.
1717 Arch Street, Suite 1320
Philadelphia, PA 19103
215-587-0003
Sileski@kgdlaw.com
RED FLAG RULES

What are the Red Flag Rules?

- The Red Flag Rules (the “Rules”) are a body of regulations drafted by six federal agencies and administered by the Federal Trade Commission. The Red Flag Rules stem from the 2003 Fair and Accurate Credit Transactions Act.
- The Rules mandate that anyone considered a “creditor” and holding a “covered account” put in place a written Identity Theft Prevention Program (“ITPP”).
- Periodic training in connection with the ITPP is also a requirement of the Rules.
The term “creditor” means “any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.”

A covered account is an account that a creditor offers or maintains primarily for personal, family, or household purposes that permits deferred payments for products or services and any other account for which there is a reasonably foreseeable risk to customers (or patients) of identity theft.
Why do the Rules apply to some medical or dental practices?

- The Practice essentially extends or facilitates the extension of credit when it:
  - Accepts credit or debit cards for the payment of services;
  - Works with financing companies to facilitate payments or payment plans by patients;
  - Bills patients for co-pays or self-pays (to cover a deductible or non-covered services);
  - Retains credit card information for unpaid sums or recurring costs for items or services.
IDENTITY THEFT

OVERVIEW

- Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crime.

- Similarly, health insurance policy information (benefits card, etc.) is also another area of identity theft that costs countless millions in fraudulent payments by insurance companies and drives up the cost of health care across the country.
IDENTIFYING RED FLAGS

- Red Flags are patterns, practices, or specific activities that indicate the possible existence of identity theft in connection with a patient account.
The Program Liaison or Administrator is responsible for:

- Updating the ITPP;
- Conducting periodic training;
- Acting as Liaison between the Board of Directors and employees;
- Serving as the second line of defense against identity theft.

The first line of defense against identity theft is the front desk employee! The Program Liaison can only react to information and detection after the fact.
WHEN TO DETECT RED FLAGS

- Opening new patient accounts:
  - Picture ID
  - Review all documentation, signature, etc.
  - Check contact information and independently contact the patient (e.g. confirming an appointment, etc.)
IDENTIFYING RED FLAGS

- Situations that involve the following Red Flags should be brought to the attention of the Program Liaison as soon as possible:
  - Notification and warnings from credit card or financing agencies;
  - Suspicious documents;
  - Suspicious identifying information;
  - Unusual use of, or suspicious activity related to, a patient account;
  - Alerts from patients, law enforcement, etc.
WHEN TO DETECT RED FLAGS

- Existing patient accounts:
  - Picture ID;
  - Review all documentation, signature, etc.
  - Check contact information and independently contact the patient (e.g. confirming an appointment, etc.);
  - When reviewing information already in the patient record, allow the patient to state the information and the employee should confirm the accuracy of the information, not the other way around!
WHEN TO DETECT RED FLAGS

- Existing patient accounts:
  - Verify changes in credit card or debit card information and **never** review such information via telephone (e.g. reading the numbers to a “patient”);
  - Verify the validity of requests to change billing information by independently contacting the patient (e.g. call back later or the following day to confirm the change);
  - Verify changes in insurance identification information given for billing and payment purposes.
PREVENTING AND MITIGATING IDENTITY THEFT

- Prevent and Mitigate:
  - Monitor suspect accounts;
  - Stay in contact with the patient;
  - Reopen account with a new number;
  - Work with the insurance company or law enforcement;
  - Always notify the Program liaison first.
As the employee is the first line of defense against identity theft for the patient, every employee should practice the following:

- Strictly follow the Practice document retention and destruction policies;
- Protect passwords;
- Keep offices and work stations clear of papers containing patient information, financial data, etc.
AREAS OF EXPOSURE

- New patient forms
- Health insurance billing documents, telephone verification, etc.
- Copying of identification, insurance cards, etc.
- Retention of credit card information and authorization for charges
- Payment of co-pays, service or item fees (e.g. checks contain account numbers and routing numbers, etc.)
RED FLAGS SUMMARY

- The ITPP depends on the employees’ ability to:
  - Detect Red Flags;
  - Respond properly and timely;
  - Stay alert;
  - Stay involved.
Questions?

- Any questions?
- Thank you for attention and being a great audience.