

NEW “RED FLAGS RULES” APPLY TO PHYSICIAN PRACTICES

By: Steven I. Kern, Esq.*

INTRODUCTION

The Federal Trade Commission has promulgated rules requiring physicians to implement written policies to help prevent identity theft. Any physician’s office that extends, renews or continues credit for a patient (i.e., any practice that bills patients for services rendered) is subject to the Red Flags Rules (the “Rules”). Even if you first bill an insurance carrier, if you ultimately bill a patient for any portion of a bill, you are considered a creditor subject to the Rules. The Rules will be enforced beginning on June 1, 2010. In addition to the Federal Rules, New Jersey and New York have their own rules pertaining to identity theft. This article addresses both Federal and State Rules. A template which will assist you in developing the identity theft prevention program required by both the FTC and the States of New Jersey and New York follows.

THE FEDERAL RED FLAGS RULES

In order to comply with the Rules you must develop a program that allows you to:

1. Identify relevant Red Flags;
2. Detect Red Flags;
3. Prevent and mitigate identity theft; and
4. Update your program periodically.

Your program must spell out how your program will be administered, and must be appropriate to the size and complexity of your practice. It must be approved by your Board of Directors, or if your practice does not have a Board, by a senior employee.

What is a “Red Flag”?

A red flag is basically something that should alert your practice to suspicious activity that may indicate identity theft. The FTC guidelines identify five categories of warning signs that must be identified and addressed:

1. alerts, notifications, or warnings from a consumer reporting agency or a service provider (a service provider is a person or entity which performs services on your covered accounts);
2. suspicious documents;
3. suspicious personal identifying information;
4. suspicious activity relating to a covered account; and
5. notices from customers, victims of identity theft, law enforcement authorities or other entities about possible identity theft in connection with covered accounts.

How are “Red Flags” Detected?

Red Flags may be detected when you verify a patient’s identity, review medical records, verify insurance forms, or receive alerts or information of suspicious activity from outside agencies.

How do I Prevent and Mitigate Identity Theft?

You must develop a written program to include appropriate responses to Red Flags, in order to prevent and mitigate identity theft. Among the actions you may take are increased monitoring of accounts, contacting the payor, contacting law enforcement agencies, changing account numbers to prevent misuse, or a combination. Preventive action may be also required if there has been a breach or attempted breach of your database.

How Often Must I Update My Program?

The Rules simply require that you update it “periodically”. However, your program should specify that it will be updated periodically to reflect changes in risks to patients resulting from changes in the methods used to engage in identity theft.

How Must the Program be Administered?

Your program must describe how it will be administered, including how you will get the approval of your management, maintain the program, and keep it current. It must also provide that the Board or designated senior employee approve any material changes to the program. The program should include appropriate staff training and a way to monitor staff to assure that they are all following the program. Administration requires continuing oversight of the program, assuring that the program remains current and relevant as methods of identification theft change. Put another way, writing a program and putting it on a shelf to collect dust is not an acceptable program.

If you engage another person or entity to perform services on your covered accounts (a service provider), you must also take steps to ensure that their activities are conducted using a reasonable identity theft prevention program. This could be done through a written contract with the service provider or by amending an existing HIPAA Business Associate Agreement.

Are There Additional State Laws that Must be Considered?

Yes. Many states have their own rules which must also be implemented as part of your identity theft prevention program. You must determine whether your state has such rules and, if so, incorporate them into your identity theft prevention program.

What are the Penalties for Noncompliance?

A violation of the Red Flags Rules can subject your practice to significant civil monetary penalties.

The new Red Flags Rules place yet another burden on medical practices, many of which are already struggling to survive under increased regulatory pressure, reduced reimbursement and increased costs. Hopefully this article, and the template which follows, will assist physicians in reducing this new burden.

NEW JERSEY'S RULES

New Jersey's Identity Theft Prevention Act ("ITPA") sets forth the duties of businesses that are subject to the provisions of the ITPA regarding breach of security, as well as treatment of Social Security numbers. The ITPA's regulations governing breach of security apply to any entity which does business in New Jersey that compiles or maintains computerized records that include personal information on New Jersey residents.

Those provisions of the ITPA regulations that have already been adopted include restrictions on the communication of Social Security numbers. Additional regulations dealing with breach of security are in pre-proposal form. Please consider the New Jersey Addendum, which follows the Program template, if you practice in New Jersey.

NEW YORK'S RULES

New York State has adopted rules affecting release of social security numbers and breaches of security as part of the New York Social Security Number Protection Law and the General Business Law. Please consider the New York Addendum, which follows the Program template, if you practice in New York.