The "Red Flags" Rule: What Health Care Providers Need to Know About Complying with New Requirements for Fighting Identity Theft

by Tiffany George and Pavneet Singh

The expression "red flag" signals "Danger: Be alert to problems ahead." For millions of consumers every year, identity theft is more than a threat — it's their reality. Businesses often bear the biggest part of the monetary damage from identity theft. But the economic, psychological, and emotional harm to victims can be devastating. And when the identity theft involves health information, the consequences can be particularly severe.

It's everyone's responsibility to do what they can to fight identity theft. Health care providers can be the first to spot the red flags that signal the risk of identity theft, including suspicious activity indicating that identity thieves may be using stolen information like names, Social Security numbers, insurance information, account numbers, and birth dates to open new accounts or get medical services.

Under the Red Flags Rule, which went into effect on January 1, 2008 *, certain businesses and organizations — including many doctor's offices, hospitals, and other health care providers — are required to spot and heed the red flags that often can be the telltale signs of identity theft. To comply with the new Red Flags Rule — enforced by the Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) — you may need to develop a written "red flags program" to prevent, detect, and minimize the damage from identity theft.

Are you covered by the Red Flags Rule? If so, have you put into place the new procedures the Rule requires?

Who Must Comply

Although every business or organization with an ongoing relationship with consumers should keep an eye out for the possibility of identity theft, health care providers should pay particular attention to the requirements that the Red Flags Rule applies to "**creditors**." To determine if your business or organization is covered by the Rule and required to develop a written identity theft Program, you'll need to answer two questions:

1. Is your business or organization either a "**creditor**" or "**financial institution**," as those terms are defined in the Rule?
2. If so, do you have "**covered accounts**"?

Although its unlikely health care providers would fall within the definition of a "financial institution," many are "creditors" under the Rule. Your business or organization is a "**creditor**" if you regularly:

extend, renew, or continue credit;

arrange for someone else to extend, renew, or continue credit; or

are the assignee of a creditor who is involved in the decision to extend, renew, or continue credit.

Under the Rule, "credit" means an arrangement by which you defer payment of debts or accept deferred payments for the purchase of property or services. In other words, payment is made after the product was sold or the service was rendered. Even if you're a non-profit or government agency, you still may be a creditor if you accept deferred payments for goods or services.

Health care providers are creditors if they bill consumers after their services are completed. Health care providers that accept insurance are considered creditors if the consumer ultimately is responsible for the medical fees. However, simply accepting credit cards as a form of payment does not make you a creditor under the Rule.

If you determine you're a creditor, the next step is to see if you have "**covered accounts**." There are two types of covered accounts. One is an account used mostly for personal, family, or household purposes that involves multiple payments or transactions. This includes continuing relationships with consumers for the provision of medical services.

The other is one for which there is a foreseeable risk of identity theft. In determining whether you have such an account, consider the risks associated with how the accounts may be opened or accessed — i.e. what type of interaction and documentation is required — as well as your experience with identity theft.

If your business or organization is a financial institution or creditor, but does not have any covered accounts, you don't need a program. But if you have covered accounts, you must develop a written program to identify and address the red flags that could indicate identity theft.

How to Comply

The Rule doesn't tell you specifically what your red flags program must look like. Instead, it gives you flexibility to implement a program that best suits your business or organization, as long as it meets the Rule's requirements.

Your starting point for developing a program is the Guidelines issued with the Red Flags Rule, available at www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf. (The Guidelines are on pages 63773-63774 of the document.) The Guidelines list the issues you must consider in developing and maintaining a program appropriate for your business or organization. You also should draw on your own experience and knowledge about identity theft risks in developing your program.

There are four basic steps to designing a program to comply with the Rule:

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

In addition, your program must spell out how it will be administered. The program should be appropriate to the size and complexity of your company or organization, as well as the nature of your operations.

Identify Relevant Red Flags

Under the Rule, creditors and financial institutions with covered accounts must develop a written program to identify the warning signs of identity theft.

The Guidelines describe the following categories of warning signs — red flags — that your program must identify and address:

alerts, notifications, or warnings from a consumer reporting agency;

suspicious documents;

suspicious personally identifying information;

suspicious activity relating to a covered account; or

notices from customers, victims of identity theft, law enforcement authorities, or other entities about possible identity theft in connection with covered accounts.

When identifying red flags, consider the nature of your business and the type of identity theft to which you might be vulnerable. Because health care providers may be at risk for medical identity theft, you'll need to identify the warning signs that reflect this risk.

Detect Red Flags

Once you've identified the red flags that are relevant to your organization or business, you must establish policies and procedures to detect them in your day-to-day operations.

For example, you may spot red flags when you verify a consumer's identity, authenticate consumers, review medical records, or verify insurance information. Some red flags may seem harmless on their own, but can signal identity theft when paired with other events, say, a change of address coupled with the use of an address associated with fraudulent accounts.

Prevent and Mitigate Identity Theft

Your program must include appropriate responses to your red flags to prevent and mitigate identity theft. These responses could include monitoring accounts, contacting the insurance provider, changing account numbers to prevent misuse, or a combination. Sometimes you may determine that no response is necessary. In other cases, certain events — such as a recent data breach, a phishing fraud that targeted your business or organization, or another suspicious activity — may raise the risk of identity theft and require specific preventive actions.

Update Your Program Periodically

Because identity theft threats change, your program must describe how you will update it to ensure that you are considering new risks and trends.

Administering Your Program

No matter how good your program looks on paper, the true test is how it works. 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.

According to the Rule, your program must be approved by your Board of Directors or, if your business or organization doesn't have a Board, by a senior employee. The Board or designated senior employee also must approve any material changes to the program. Your program should include staff training as appropriate, and provide a way for you to monitor the work of your service providers. The keys are to maintain oversight of the program, keep it relevant and current, and ensure that all necessary members of your staff — from the intake desk to the records room — are on board. A program that stays in a filing cabinet isn't a good program.

Penalties for Noncompliance

Although there are no criminal penalties for failing to comply with the Red Flags Rule, financial institutions or creditors that violate the Rule may be subject to civil monetary penalties. But there's an even more important reason for compliance: It assures your consumers that you are doing your part to fight identity theft.

Have questions about how health care providers can comply with the Rule? Email RedFlags@ftc.gov.

*On October 22, 2008, the Federal Trade Commission issued an Enforcement Policy statement that delays enforcement of the Red Flags rule until May 1, 2009 (http://www.ftc.gov/opa/2008/10/redflags.shtm). This does not affect enforcement of the address discrepancy and credit card issuer rules. Nor does it affect compliance for entities not under the jurisdiction of the Commission.

Tiffany George and Pavneet Singh are attorneys in the Federal Trade Commission's Division of Privacy and Identity Protection.

Physician Legal Alert: New "Red Flag Rules" & Physician Practices

By: Michael J. Schoppmann, Esq.
Kern Augustine Conroy & Schoppmann, P.C.

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 Flag 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 takes effect on May 1, 2009.

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. The healthcare law firm of Kern Augustine Conroy & Schoppmann, P.C. has developed a free template available on its website to assist you in developing your own program: It can be found at www.drlaw.com.

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 four categories of warning signs that must be identified and addressed:

1. alerts, notifications, or warnings from a consumer reporting agency;
2. suspicious documents;
3. suspicious personally identifying information; and
4. suspicious activity relating to a covered account; or 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 requires that you update it "periodically". However, your program should specify that it will be updated when the methods of identity theft threats change or new risks and trends develop.

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.

What are the Penalties for Noncompliance?

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

These new Red Flag 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 guide, and the free template available through Kern Augustine Conroy & Schoppmann, P.C., will assist physicians in reducing this new burden.

Kern Augustine Conroy & Schoppmann, P.C., Attorneys to Health Professionals, www.drlaw.com, has offices in New York, New Jersey, Florida, Pennsylvania and Illinois. The firm's practice is solely devoted to the representation of health care professionals. Mr. Schoppmann may be contacted at 1-800-445-0954 or via email - schoppmann@drlaw.com.

RED FLAGS RULE

FOR THE MEDICAL PRACTICE

Kern Augustine Conroy & Schoppmann, P.C.

www.drlaw.com

Kern Augustine Conroy & Schoppmann, P.C., has prepared these materials for your use in complying with the Federal Trade Commission's (FTC) Red Flags Rule. The FTC will begin enforcing this Rule on May 1, 2009. As discussed in the following article, your practice may need to develop a written Identity Theft Prevention Program. You should review the article, as well as the FTC's Red Flags Rule Guidelines, to determine if the Red Flags Rule applies to your practice.[1] If it does, you may use the following Identity Theft Prevention Program Template as a model which must be adapted to your practice's specific situation (size, operations, experience with identity theft, etc.). Following the model template you will find New York state law addenda containing state regulations that affect your Identity Theft Prevention Program. These should be incorporated into your Program, as applicable. Please note that there are significant provisions in the recently enacted American Recovery and Reinvestment Act of 2009 which, when fully implemented, will also affect provisions of both your Identity Theft Prevention Program and your HIPAA Privacy and Security Programs. Note: The templates which follow are provided to assist you in meeting your obligations under the Red Flags Rule and State Law. They are not offered as legal opinion, and should not be adapted to your practice without the assistance of experienced health-law legal counsel.

[1] The Guidelines can be accessed at:www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf at pages 63773-63774.

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 May 1, 2009. In addition to the Federal Rules, New York has adopted its 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 State of 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 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.

[PRACTICE]

IDENTITY THEFT PREVENTION PROGRAM TEMPLATE

ADOPTED AND EFFECTIVE:

UPDATED:

I. Adoption of Identity Theft Prevention Program

[Practice] ("the Practice") developed this Identity Theft Prevention Program ("the Program") pursuant to the Federal Trade Commission's Red Flags Rule ("the Rule"), 16 *C.F.R.* §681.2. The Program was developed with the oversight and approval of the Practice's [Board of Directors/Managing Partner/Managing Member] who has determined that our Practice is a Creditor with Covered Accounts (as defined below) and is obligated to comply with the Rule. After due consideration of the Rule's requirements and its guidelines (and including in the Program those guidelines in Appendix A of the Rule that are appropriate), and of the size and complexity of the Practice's operations and systems, and the nature and scope of the Practice's activities, the [Board/Managing Partner/Managing Member] determined that this Program is reasonable and appropriate for the Practice and, therefore, approved this Program on the ___ day of _____, 2009.

II. Program Purpose and Definitions

A. Fulfilling the Obligations of the Rule

Under the Rule, every "Creditor" with "Covered Accounts" is required to establish an Identity Theft Prevention Program tailored to the size, complexity and nature of its operations. The Program must contain policies and procedures reasonably designed to:

1. Identify relevant "Red Flags" for new and existing "Covered Accounts" and incorporate those Red Flags into the Program.
2. Be able to detect Red Flags that have been incorporated into the Program.
3. Respond appropriately to any Red Flags that are detected in order to prevent and mitigate "Identity Theft."
4. Update the Program periodically to reflect changes in risks to our patients and to the safety and soundness of our Practice from Identity Theft.

B. Definitions of Terms used in the Program

Account means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes, including an extension of credit.

A Covered Account is:

i. an account that a creditor offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions; and
ii. any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers (our patients) of, or to the safety and soundness of the creditor from, identity theft.

Credit is an arrangement by which a person or entity defers payment of debts or accepts deferred payments for the purchase of services or property.

A Creditor is any person or entity who:

i. regularly extends, renews or continues credit;
ii. regularly arranges for the extension, renewal or continuation of credit; or
iii. any assignee of an original creditor who participates in the decision to extend, renew or continue credit.

Identifying Information is defined under the Rule as any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including name, address, telephone number, social security number, date of birth, government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internal Protocol Address, or routing code.

Identity Theft is fraud committed using the identifying information of another person, which can be medical identity theft and/or financial identity theft.

Program Administrator is the Practice's administrative personnel charged with the implementation of the Program (which may be one or more persons and may be the Practice's HIPAA Privacy Officer).

Red Flag means a pattern, practice or specific activity that indicates the possible existence of identity theft in connection with a covered account.

Service Provider means a person or entity that provides a service directly to a creditor.

III. Policies and Procedures

A. Identification of Red Flags

Because our Practice regularly extends Credit to patients by establishing an account that permits multiple payments, our Practice is a Creditor offering Covered Accounts. Commentary to the Rule states that "creditors in the health care field may be at risk of medical identity theft (i.e., identity theft for the purpose of obtaining medical services) and, therefore, must identify Red Flags that reflect this risk."

In order to identify relevant Red Flags, our Practice considers the types of accounts it offers and maintains, the methods it provides to open its accounts, the methods it uses or provides to access its accounts, and its previous experience with Identity Theft. The Practice has identified the following Red Flags for our Program:

1. Alerts, Notifications and Warnings Received from Consumer Reporting Agencies or Service Providers of the Practice

    a. Report of fraud or other alert accompanying a credit or consumer report
    b. Notice of a credit freeze in response to a request for a consumer report
    c. Report, such as from one of our Service Providers, indicating a pattern of activity that is inconsistent with the history and usual pattern of activity of a patient account

2. Suspicious Documents

    a. Identification document that physically appears to be forged, altered or otherwise not authentic
    b. Identification document on which a person's photograph or physical description is not consistent with the person presenting the document
    c. A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance (unless the Practice can confirm that there is a legitimate reason for the absence of such documentation)
    d. Other document containing information that is not consistent with existing patient information (such as if a person's signature appears forged, based on previous instances of the person's signature on file)

3. Suspicious Personal Identifying Information

    a. Identifying information presented that is inconsistent with other information the patient provides (e.g., inconsistent birth dates)
    b. Identifying information presented that is inconsistent with other sources of information (e.g., an identification number presented that does not match a number on the person's insurance card)
    c. Identifying information presented that is the same as information shown on other documents that were found to be fraudulent
    d. Identifying information presented that is consistent with fraudulent activity (e.g., invalid phone number or fictitious billing address)
    e. Identifying information presented that is the same as information provided as identifying information by another patient
    f. A patient fails to provide complete identifying information on any patient information form when reminded to do so and the Practice is not prohibited by law from requiring the information be provided
    g. A patient provides identifying information that is not consistent with the information the Practice has on file for the patient

4. Suspicious Account or Medical Record Activity

    a. Payments stop on an otherwise consistently up-to-date account
    b. Mail sent to the patient is repeatedly returned as undeliverable
    c. Breach in the Practice's computer system security
    d. Unauthorized access to or use of Covered Account information
    e. Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient, e.g., discrepancies in age, race, blood type or other physical descriptors

5. Alerts from Others

    a. A complaint or question from a patient based on the patient's receipt of:
        i. A bill for another individual
        ii. A bill for a product or service that the patient denies receiving
        iii. A bill from a health care provider that the patient never patronized
        iv. A notice of insurance benefits or Explanation of Benefits for health services never received
    b. A complaint or question from a patient about the receipt of a collection notice from a bill collector

c. A complaint or question from a patient about information added to a credit report by the Practice or the patient's insurer
d. A dispute of a bill by a patient who claims to be the victim of any type of Identity Theft
e. A patient or insurance company report that coverage for legitimate medical services is denied because insurance benefits have been depleted or a lifetime cap has been reached
f. A notice or inquiry from an insurance fraud investigator regarding a patient's account (which could indicate internal or external Identity Theft)
g. A notice or inquiry from a law enforcement agency regarding possible Identity Theft in connection with a Covered Account held by the Practice
h. A notice from a victim of Identity Theft regarding possible Identity Theft in connection with a Covered Account held by the Practice

B. Detecting Red Flags

1. New Accounts – In order to detect any of the Red Flags identified above associated with the opening of a new Covered Account, Practice personnel will take the following steps to obtain and verify the identity of the person opening the account:

   a. Require certain identifying information such as: name, date of birth, residential or business address, insurance card, employer name and address, driver's license or other identifying information.
   b. Actually verify the patient's identity by reviewing the identifying information presented and contacting the patient's insurer, if appropriate.

2. Existing Accounts – In order to detect any of the Red Flags identified above for an existing account, Practice personnel will take the following steps to monitor the transactions and activity on an account, in compliance with our Practice's HIPAA Privacy policies and procedures:

   a. Verify the identification of a patient who requests information (in person, via telephone, via facsimile, via email)
   b. Verify the validity of requests to change a billing address
   c. Verify changes in credit card or other information given for purposes of billing and payment

C. Preventing and Mitigating Identity Theft

In the event Practice personnel detect any identified Red Flags, the Practice shall take one or more of the following steps, depending on the Red Flag detected and on the degree of risk posed by the Red Flag:

1. Prevent and Mitigate

a. Notify the Program Administrator who may determine it is necessary to contact the Practice's legal counsel for determination of the appropriate step(s) to take
b. Comply with state and federal requirements related to a breach of computer security
c. Contact the patient, in compliance with applicable law
d. Notify law enforcement, in compliance with applicable law
e. Continue to monitor an account for evidence of Identity Theft
f. Change any passwords or other security devices that permit access to a Covered Account
g. Not open an account for a new patient if a Red Flag is detected in relation to such account
h. Place a hold on further transactions related to an account for which a Red Flag has been detected
i. Not attempt to collect on an account
j. Determine that no response is warranted under the circumstances

2. Protect Patients' Identifying Information

The Practice's HIPAA Privacy and Security Program will be utilized, and updated along with this Program, if necessary, to further prevent the likelihood of Identity Theft occurring with respect to Practice accounts.

3. Protecting and Correcting Medical Information

If our Practice determines that medical Identity Theft has occurred, there may be errors in the patient's chart as a result. Fraudulent information may have been added to a pre-existing chart, or the contents of an entire chart may refer only to the health condition of the identity thief, but under the victim's personal identifying information. In such cases, our Practice shall take appropriate steps to avoid mistreatment due to the fraudulent information, such as file extraction, cross-referencing charts, etc.

D. Program Updates

The Program Administrator will periodically, but no less than annually, review and update this Program to reflect changes in risks to patients and the soundness of the Practice in protecting against Identity Theft, taking into consideration the Practice's experience with Identity Theft occurrences, changes in methods of how Identity Theft is being perpetrated, changes in methods of detecting, preventing and mitigating Identity Theft, changes in the types of accounts the Practice offers, and changes in the Practice's business relationships with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program are warranted. The Program Administrator will present any recommended changes to the [Board/Managing Partner/Managing Member], which will make a determination whether to accept, modify or reject the recommended changes to the Program.

IV. Program Administration

A. Oversight of the Program

The Practice [Board of Directors/Managing Partner/Managing Member] is responsible for the development, implementation and updating of this Program and will approve the initial Program, as well as any updates. The Program Administrator is responsible for taking steps to ensure appropriate training of Practice personnel regarding the Program, receipt and review of reports regarding the detection of Red Flags, determining (with the assistance of the Board/Partner/Member and/or legal counsel) the steps for preventing and mitigating Identity Theft when a Red Flag is detected, and recommending updates to the Program.

B. Staff Training and Reporting

Practice personnel whose role requires their participation in implementing the Program will be trained by or under the direction of the Program Administrator. Training shall cover the Red Flags identified in the Program, detecting Red Flags, and reporting and responding to detected Red Flags. The Program Administrator shall report annually to the [Board/Partner/Member] on the Practice's compliance with the Rule in terms of effectiveness of addressing Identity Theft, service provider arrangements, significant incidents involving Identity Theft and the Practice's response, and recommendations for material changes to the Program.

C. Oversight of Service Provider Arrangements

The Practice will require, by written contract, that service providers that provide services or perform activities on our Practice's behalf in connection with a Covered Account have policies and procedures in place designed to detect, prevent and mitigate the risk of Identity Theft in regard to the Covered Accounts. If the service provider is a HIPAA Business Associate of the Practice, the Business Associate Agreement with that service provider shall be amended to incorporate the above requirements.

V. State Laws and Regulations

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.

New York Addendum

Note: In addition to complying with federal identity theft prevention regulations, medical practices are required to comply with New York State consumer protection laws. These laws include criminal statutes that define identity theft and the unlawful possession of personal information as well as laws that define how to safeguard Social Security Numbers and explain what to do in the event of an inadvertent unauthorized disclosure. The following should, where applicable, be included in your identity theft prevention program:

In order to comply with The New York Social Security Number Protection Law (N.Y. Gen. Bus. Law § 399-dd) our Practice will not do the following with regard to a social security account number[2]:

1. Intentionally communicate to the general public or otherwise make available to the general public in any manner an individual's social security account number;
2. Print an individual's social security account number on any card or tag required for the individual to access products, services or benefits provided by our Practice;
3. Require an individual to transmit his or her social security account number over the internet, unless the connection is secure or the social security account number is encrypted;
4. Require an individual to use his or her social security account number to access an internet web site, unless a password or unique personal identification number or other authentication device is also required to access the internet website.
5. Print an individual's social security account number on any materials that are mailed to the individual, unless state or federal law requires the social security account number to be on the document to be mailed. Notwithstanding this paragraph, social security account numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the social security account number. A social security account number that is permitted to be mailed under this section may not be printed, in whole or part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.
6. Encode or embed a social security number in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, or other technology, in place of removing the social security number as required by this section.

[2] "Social security account number" shall include the number issued by the federal social security administration and any number derived from such number but not any number that has been encrypted.

7. File any document available for public inspection with any state agency, political subdivision, or in any court of this state that contains a social security account number of any other person, unless such other person is a dependent child, or has consented to such filing, except as required by federal or state law or regulation, or by court rule.

This does not prevent our Practice's collection, use, or release of a social security account number as required by state or federal law, the use of a social security account number for internal verification, fraud investigation or administrative purposes or for any business function specifically authorized by law.

Our Practice will take reasonable measures to ensure that no employee has access to a social security number for any purpose other than for a legitimate or necessary purpose related to the conduct of our Practice and will provide safeguards necessary or appropriate to preclude unauthorized access to the social security account number and to protect the confidentiality of such number.

In order to comply with The New York State General Business Law § 899-aa, which outlines how our Practice should respond in the event of the breach of security of our computerized data system, our Practice will:

1. Disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York State whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made as provided in paragraph 4, below, in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system;
2. Notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization;
3. Potentially delay any necessary notification if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required shall be made after such law enforcement agency determines that such notification does not compromise such investigation;
4. Directly provide any required notice to the affected persons by one of the following methods:
   (a) written notice;
   (b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by our Practice in such form; provided further, however, that in no case shall our

Practice require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction with our Practice;

(c) telephone notification provided that a log of each such notification is kept by our Practice; or

(d) substitute notice after demonstrating to the state attorney general the necessary requirements;

5. Ensure that any required notice shall include contact information for our Practice and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired; and
6. Ensure that:

   (a) In the event that any New York residents are to be notified, the Practice shall notify the state attorney general, the consumer protection board, and the state office of cyber security and critical infrastructure coordination as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents; and that

   (b) In the event that more than five thousand New York residents are to be notified at one time, the Practice shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.