

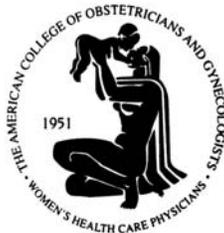
**FTC IDENTITY THEFT
RED FLAGS RULE**

PROGRAM MANUAL

A How-To Guide for Your Medical Practice

provided by

the American College of Obstetricians and Gynecologists



This manual has been prepared to provide the reader with information on the Federal Trade Commission's Identity Theft Red Flag Rules. The manual is being provided with the understanding that the American College of Obstetricians and Gynecologists (ACOG) is not engaged in rendering any legal, accounting or other professional service through this manual. The materials contained in the manual have been prepared by ACOG employees based on information obtained from the American Medical Association, the Federal Trade Commission, and the American Urological Association, Inc. The manual is not intended to be, and should not be used as, a substitute for seeking professional services or advice.

This manual is provided free of charge to ACOG members. **Duplication of this manual for use outside of the medical practices of ACOG members is strictly prohibited.**

DISCLAIMER

IMPORTANT DISCLAIMER REGARDING THE LAWS OF YOUR STATE:

Many state privacy laws as well as the Healthcare Insurance Portability and Accountability Act (HIPAA) rules will continue to apply following the May 1, 2009 compliance deadline of the Red Flags Rule. This manual does not include a review of HIPAA regulations, state laws or other regulations that may apply to protect the Privacy and Security of confidential patient information used by your practice. The form documents and agreements provided in this manual do **NOT** necessarily meet the requirements of your state's laws.

You are advised to consult with your state medical society, local chapter of specialty society, legal counsel or advisors familiar with your state's laws to determine which state laws and regulations will impact: (1) the operation of your practice, and (2) the contents of any form, template document or agreement contained in this manual.

This manual should be used only as a general reference and guide for outlining specific steps that you may take in order to comply with certain regulations issued pursuant to the Federal Trade Commission Red Flags Rules. The steps contained in this manual are general examples and should serve only as suggested starting points in your practice's compliance with the Red Flags Rules. You may alter the formatting, typeset, organization and fonts size of the manual as long as the integrity or substance of the manual is maintained.

Table of Contents

Overview of Red Flags Rule	Page 5
Risk Assessment Form	Page 8

Policies and Procedures

Reacting to alerts and notifications	Page 10
Reacting to receipt of suspicious documents	Page 11
Obtaining personal ID information	Page 13
Reacting to suspicious use or activity re: covered accounts	Page 15
Reacting to requests or complaints	Page 17
Employee training	Page 18

Appendix I

Sample Reception Room information and telephone script	Page 19
--	---------

Overview of Red Flags Rule

Most medical practices have been declared “creditors” in the judgment of the Federal Trade Commission (FTC) and are therefore subject to compliance with the Red Flags Rule (16 CFR 681.2). The information contained in this Manual is intended to assist your practice in developing policies and procedures to carry out this compliance and to train your employees on the Red Flags Rule and the steps you have elected to take toward compliance. The red flags referred to in the title of the rule are the indicators that help indicate the possibility of, and thereby prevent, identity theft.

Purpose of the Rule

The Red Flags Rule was promulgated by the FTC to protect individuals who are granted credit from identity theft. Identity theft can be defined as the act of unlawfully obtaining personal identifying information of an individual and using it for fraudulent reasons. Fraudulent use includes patients using someone else’s medical insurance to pay for treatment. Another example would be theft and/or use of patients’ credit information by employees of the practice. Especially since the advent of use of the Internet to transmit this type of data among authorized parties, identity theft has resulted in the loss of billions of dollars each year to businesses and individuals. The Red Flags Rule require all creditors or financial institutions that maintain information for which there is a risk of identity theft to implement a program designed to protect that information to the extent practical in the particular setting.

Although most ob/gyn practices do not officially extend credit involving examining financial status and charging interest on unpaid balances, the FTC has deemed the act of allowing patients to make deferred payments after insurance policy benefits have been collected as having established a creditor relationship between the practice and the patient.

Implementation Deadline

The deadline for implementation of Red Flags Rule policies and procedures by healthcare providers is May 1, 2009. The law governing compliance with the Red Flags Rule is the Fair and Accurate Credit Transactions Act of 2003 (FACTA).

The Red Flags Rule aligns with the HIPAA Privacy, Security and Transactions Rules by incorporating protection of confidential financial information along with private health information. In certain instances, a reference to your practice’s policies and procedures that assist you in complying with HIPAA may be sufficient to address issues associated with the Red Flags Rules.

Penalties for failure to comply

Penalties for failure to comply with the Red Flags Rule will normally be assessed in the event of a knowing violation. Although the FTC has not identified or described any enforcement activities at this time, it is reasonable to assume that enforcement activities will be initiated on the basis of patient complaints. Penalties imposed by FTC for violations may not be greater than \$2,500 per violation. Therefore, it is critically important to alert your patients and the parties responsible for payment of your fees for services that you have Red Flags Rule policies and procedures in place. This can be accomplished by means of signs in your reception area, recorded messages on your telephone-hold systems, advisories on your patient statements, etc. Examples of these advisories are provided in **Appendix I** of this Manual.

Flexibility of policies and procedures

Like many other compliance programs applicable to healthcare providers, the Red Flags Rule allows an ob/gyn practice to design a program that fits effectively into day-to-day operations. The Rule makes it clear that your practice may incorporate existing activities designed to protect private information into this effort to protect your patients from identity theft. In adopting your Red Flags Rule program, consider the technology available to your practice, the business acumen of your employees and physicians, the routine activities undertaken by your practice that exposes your patients and their responsible parties to risk of identity theft. Implement procedures that can be easily trained and can quickly become habits for your staff as they interact with patients in the normal course of your business. Remember that your responsibility is to sincerely attempt to reduce the risk of identity theft. In the event a theft occurs, despite your best efforts, your practice is expected to document that activity, issue proper notification to your patient and to authorities, and to modify your procedures to reduce the risk of a repeat problem.

Categories of Red Flags

The following are the five categories of Red Flags identified by FTC that should be considered by your practice. Some of these categories would normally not apply to your practice. In those cases, simply documenting that your team has assessed the risk and found it negligible is all that is necessary to comply. Other categories may clearly pose a risk to your patients. You should implement procedures to reduce the risk. The five categories of Red Flags are:

- Alerts, notifications or warnings from a consumer reporting agency – Most ob/gyn practices would not routinely obtain credit reports on their patients. However, for some uninsured patients or those with high-deductible health plans, the use of credit reporting may become necessary.
- Suspicious documents – For example, a request for copies of medical records from a health care provider or attorney with which your practice staff is not familiar.
- Suspicious personal identifying information – The Red Flags Rule requires health care providers to undertake a major additional step in processing patient encounters. This is probably the most important function to be incorporated into the policies and procedures for a medical practice. It is important to verify the identity of patients visiting your practice and to identity of patients calling to request personal information.
- Unusual use of, suspicious activity relating to a covered account – For example, a patient requests that you take a credit card payment over the phone or you accept a credit card at your facility that does not have the patient’s name on it.
- Notices from patients, law enforcement authorities or other businesses about possible identity theft in connection with covered accounts.

Conducting a Risk Assessment

In addition to the paperwork involved in establishing your practice’s Red Flags Rule compliance program, it is important that you document that your practice leadership has assessed the degree of risk of identity theft that your patients might face in interacting with your practice for medical care. The simplest way to conduct such a risk assessment is to focus on each of the five risk categories listed above and consider where any risks for misappropriation could occur. Those areas that are determined to be high risk are the ones where drafting of procedures and staff training are essential. Areas evaluated as low risk may be dealt with by simply documenting that the practice leadership has determined that other procedures associated with the HIPAA regulation compliance sufficiently address the risks involved for identity theft. The Risk Assessment Documentation Form on the following page can be used to guide and document your discussions.

Risk Assessment Documentation Form

Practice Name: _____

Date Completed: _____

Date Approved by Board: _____

Using a scale where 1 is the lowest possible risk and 5 is the highest possible risk, assess the risk routinely faced by your patients for the following five Red Flags risk categories. Use the lines below each category to document your findings about these risks.

- Alerts, notifications or warnings from a consumer reporting agency

- Risk level _____

- Suspicious documents

- Risk level _____

- Suspicious personal identifying information

- Risk level _____

- **Unusual use of, suspicious activity relating to a covered account**

- Risk level _____

- **Notices from patients, law enforcement authorities or other businesses about possible identity theft in connection with covered accounts**

- Risk level _____

Reacting to an alert or notification from a reporting agency

Practice Name: _____

Date Completed: _____

Date Approved by Board: _____

Policy: In the event that our practice receives notice from an agency that one of our patients may be a victim of identity theft as evidenced by information contained on the patient's credit report, a designated staff member will contact the patient and review their demographic information and their outstanding account balances. This patient contact will be carried out within 15 days of receiving the notice.

Procedure:

1. A practice representative will contact the patient or the patient's responsible party by phone. Before continuing with the discussion, the caller will explain the Red Flags rule (see number 1a under "Obtaining personal identifying information" below) and verify the patient's identity by asking one or more of the following validation questions:
 - a. Patient's medical record number or Social Security Account Number or
 - b. Date of the patient's last visit to our practice and the name of the physician seen and/or
 - c. Patient's middle name, date of birth and/or
 - d. Some other identifying information contained in the medical record.
2. Once the patient's identity has been verified, the practice representative will read the content of the notice received and ask the patient if they are aware of this alert.
3. The practice representative will review the patient's demographic information and outstanding account balances that are on record with the practice. The patient should confirm whether the information on file is accurate. Any disparities may be resolved by phone or the patient may be asked to come to the office to do a more thorough review.
4. The practice representative will record a brief summary of the actions taken on the patient's electronic financial record or in a written file.

Reacting to receipt of suspicious documents

Practice Name: _____

Date Completed: _____

Date Approved by Board: _____

Policy: In the event that our practice receives documents requesting private patient information from sources not recognized by practice staff as entities involved in routine **T**reatment, **P**ayment or health care **O**perations (TPO) as defined in our HIPAA Privacy Policy, a practice representative will contact the patient and confirm that this request was authorized. This patient contact will be carried out within 5 days of receiving the notice.

Procedure:

1. A practice representative will contact the patient or the patient's responsible party by phone. Before continuing with the discussion, the caller will explain the Red Flags rule (see number 1a under "Obtaining personal identifying information" below) and verify the patient's identity by asking one or more of the following validation questions:
 - a. Patient's medical record number or Social Security Account Number or
 - b. Date of the patient's last visit to our practice and the name of the physician seen and/or
 - c. Patient's middle name, date of birth and/or
 - d. Some other identifying information contained in the medical record.
2. Once the patient's identity has been verified, the practice representative will explain the nature of the document received and identify the sender. If the document was accompanied by a signed authorization by the patient, the practice representative will verify the signature. If the document was not accompanied by a signed authorization by the patient, the practice representative will:
 - a. Decide if the information requested is related to TPO. If so, the practice representative will solicit the patient's verbal agreement to release the information requested and document this agreement.
 - b. If the information is not related to TPO, then the practice representative will advise the patient that a signed authorization is required and send the appropriate form to the patient to sign and return.

3. If the documents received are not verified by the patient, the practice representative should contact the requester and advise that no information may be released without a signed authorization by the patient. The practice representative will not divulge any patient information except that already included on the suspicious document.
4. If the practice representative becomes concerned as to the identity or motives of the requester as a result of this contact, then the appropriate practice officers should be notified for purposes of notifying proper authorities about the possibility of attempted identity theft.
5. The practice representative will record a brief summary of the actions taken on the patient's electronic financial record or in a written file.

Obtaining personal identifying information from all patients

Practice Name: _____

Date Completed: _____

Date Approved by Board: _____

Policy: Effective on the date listed above, every patient admitted for care in this practice shall present certain specified documents that will assist us in verifying the identity of the patient and verifying that the person receiving treatment is entitled to insurance benefits for which our practice is asked to submit claims. Exceptions to this identification requirement will be made for patients who would be considered emergency patients as defined under the Emergency Treatment and Active Labor Act rules with which our practice already complies.

This requirement must be met by New Patients at their first visit to any of our practice facilities where we control admittance. This requirement must be met by Established Patients at the first visit that occurs after the effective date listed above. This requirement need only be met once for each patient per calendar year unless the patient submits revisions to the demographic or insurance data we have on file. Submission of these changes will require additional proof of identity.

Procedure:

1. When calling to request an initial appointment after the effective date of this policy, each patient will be read the following statement by any practice staff who books appointments:
 - a. As a result of new requirements put into effect by the Federal Trade Commission to protect consumers from identity theft, we must require our patients to present one of the following documents for our inspection – (1) Drivers' License or another State approved Photo ID (2) Current copy of your health insurance card. In the event your Photo ID does not contain your current address, you must also present a utility bill or other document that shows your correct address. In order to avoid having you present this Photo ID every time you visit our practice, we will make a copy of it and retain it in our files so that your identity can be visually verified upon your arrival.
2. When patients that have not previously presented their personal identifying information arrive at the practice's reception desk, they will be asked to present the items listed above. The practice representative receiving these documents will carry out two steps – (1) inspect the Photo ID carefully for any alterations or forgeries (2) look carefully at the

patient to confirm that the individual facial characteristics match the photo (3) resolve any disparities using techniques listed below.

3. If the practice representative suspects any disparities, he/she should take any or all of the following confirmatory steps:
 - a. Ask the patient to provide additional identity documentation such as a credit card or business card
 - b. While holding the Photo ID in a manner that blocks the view of the patient, ask the patient to recite their data of birth and home address. Match their answers to the information on the ID.
 - c. Ask the patient to sign a blank piece of paper and match the signature to the one on the ID.
4. Inform the patient that you need to make a copy of the ID so that they will not be required to present it at every future visit. Copy the card.
5. If the practice representative continues to have suspicions, return the card to the patient but retain the copy in order to alert authorities. Advise the patient that due to your inability to confirm their identity, the Red Flags Rule requires you to alert your practice's Security Officer and perhaps local authorities. Suggest that their appointment be rescheduled until the problem can be resolved unless they can produce additional proof of their identity.
6. For future visits, the practice representative need only inspect the ID copy in the patient's record and match it to the patient's physical appearance.

Reacting to use of or suspicious activity relating to a covered account

Practice Name: _____

Date Completed: _____

Date Approved by Board: _____

Policy: The billing personnel of the practice will remain vigilant to identify any requests concerning a patient's financial account that would be considered out of the ordinary and will take steps to avoid releasing any private information that may be detrimental to the patient's credit status.

Examples of suspicious activity include:

- A phone call request inquiring about the last payment on the account and in what form it was made,
- Anyone other than the patient (whose identity has been confirmed) requesting an itemized statement,
- An unusual number of account inquiries on a single account or similar inquiries on multiple accounts from the same entity
- Frequent changes of address
- Presentation of Powers of Attorney

Procedure:

1. A practice representative receiving such requests by phone will explain the Red Flags rule (see number 1a under "Obtaining personal identifying information" above) and verify the patient's identity by asking one or more of the following validation questions:
 - a. Patient's medical record number or Social Security Account Number or
 - b. Date of the patient's last visit to our practice and the name of the physician seen and/or
 - c. Patient's middle name, date of birth and/or
 - d. Some other identifying information contained in the medical record.

2. If anyone other than the patient makes such a request or submits such documents, the practice representative will refuse the request and notify the practice's Security Officer.
3. The Security Officer will evaluate the situation and may elect to contact the patient to verify whether the suspicious activity occurred at the request of the patient.

Reacting to patient request for assistance or complaints of identity theft

Practice Name: _____

Date Completed: _____

Date Approved by Board: _____

Policy: In the event that the practice is contacted by one of our patients or a legal authority about potential identity theft, we will flag the patients account in such a way that all employees know of the possible problem so that increased vigilance and reporting of any incident will be made promptly.

Procedure:

1. A practice representative (preferably the Security Officer) will contact the patient. After confirming their identity, they will discuss the complaint and research the patient's account.
2. Documentation of all Red Flags Rule compliance activities related to the specific account will be copied and held for turning over to authorities. This includes documentation of identity verification either in person or by phone.
3. Any further discussion with any person representing themselves as a patient representative will only occur upon receipt of a signed authorization by the patient until the problem is resolved.
4. A summary of the events connected with the case will be reviewed at the next employee training session.

Employee training on Red Flags Rule

Practice Name: _____

Date Completed: _____

Date Approved by Board: _____

Policy: Employee training on the practice's Red Flags Rule policies and procedures will be carried out within 30 days of adoption of this document. Follow-up training will be incorporated into the regular employee training schedule for HIPAA, OSHA, etc. Follow-up training will take place a minimum of once per year. Spot training will occur for individual employees as prescribed by management to improve the effectiveness of Red Flags Rule compliance.

Appendix I

1. Examples of Reception Room Sign

To Our Patients:

In accordance with Federal Trade Commission requirements, effective May 1, 2009, our practice complies with the Red Flags Rule that is intended to
PROTECT YOU AGAINST IDENTITY THEFT.

We are required to ask our patients to prove their identity by showing a photo ID and by answering certain questions that only you or your family members would know when you contact us by phone. We appreciate your cooperation with our efforts to protect your identity and comply with Federal regulations.

2. Example of Telephone Script

(Making appointments for visits) Ms. Smith, Federal regulations that went into effect on May 1, 2009 require us to ask our patients to prove their identity by showing a photo ID when they visit our office. Please remember to bring your photo ID when you arrive in addition to your current health insurance card. In order to save you the trouble of showing your ID at every visit, we will make a copy of it when you present it. This way our employees can verify your identity on sight. If your photo ID does not include your correct billing address, please bring a utility bill or other document that shows both your name and address.

(Responding to telephone calls involving private information) Ms. Smith, Federal regulations that went into effect on May 1, 2009 require us to verify your identity before giving out private information about you over the phone. Please answer the following questions that only you or your family members would know. (Ask Questions from Procedure Document)

We appreciate your cooperation with our efforts to protect your identity and comply with Federal regulations.