# Physician Office Compliance with the Red Flag Rule

The Red Flag Rule, implemented by the Federal Trade Commission (FTC) on ***May 1, 2009***, requires all financial institutions and creditors, **including physician offices**, to design and implement a compliance policy appropriate to their size and complexity. The 26 examples of Red Flags are not a checklist (Attachment 1), but rather, examples that your practice may want to use as warning signs of identify theft. Again, no two practices are identical, so your compliance policy must be developed accordingly. A sample policy that can be easily customized for your practice has been developed by the American Medical Association, with information included to assist DCMS members to report cases of identify theft (Attachment 2). Furthermore, the following guidelines can be used as generic summary as to what is included in the compliance policy for addressing the FTC Red Flag Rules:

☑ Develop Red Flag Policies and Procedures for your office (Attachment 2).

☑ Review the 26 example red flags with staff and be prepared to report them to the appropriate agency as you deem necessary (Attachment 1).

☑ Recognize that Red Flag Rules are not relevant to HIPAA and require a separate, internal compliance policy.

☑ Establish an admission or "check-in" policy that requires patients to provide **both** a state photo identification (e.g., drivers license) and insurance card. Any employees involved in this process should be involved in the development of the compliance program.

☑ Ensure that the compliance policy best suits the size of your practice (i.e., risks and program complexity will be much greater for large practices and less for smaller practices).

☑ Update the policy periodically. This can be done annually along with the review and update of other internal policies (e.g., employee handbook, OSHA compliance, etc.). Make certain staff are effectively trained and informed of any changes to the policy at any time.

☑ Document approval of the new red flags policy and procedure by the Board of Directors or internal memorandum "For the Record" of the practice.

## *Filing a Complaint

The FTC, the nation's consumer protection agency, works to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers notice, stop, and avoid said practices. **To report or discuss a case of identify theft, call toll free 1-877-438-4338** or go to the FTC online, at **http://www.ftc.gov/opa/2002/02/idtheft.shtm** for more information. Medicaid fraud-related complaints should be reported to the **Florida Medicaid Fraud Control Unit at 1-866-966-7226**.

Similar to any situation whereby a patient becomes unruly or disruptive, a confrontation with a patient regarding suspected identify theft is a possibility. It is recommended that the practice contact the **Jacksonville Sheriff Office's non-emergent line (630-4722)** for assistance if uncontrollable, disruptive behavior is experienced. Of course, 911 is reserved for life-threatening emergencies.

**Additional Assistance:**

Should you still have questions or wish to identify an attorney for legal guidance, please contact Jay Millson, DCMS Executive Director, at 355-6561, ext. 105, for assistance.

**Attachment 1**

# The 26 Red Flag Rules

1. A fraud alert included with a consumer report.
2. Notice of a credit freeze in response to a request for a consumer report.
3 A consumer reporting agency providing a notice of address discrepancy.
4. Unusual credit activity, such as an increased number of accounts or inquiries.
5. Documents provided for identification appearing altered or forged.
6. Photograph on ID inconsistent with appearance of customer.
7. Information on ID inconsistent with information provided by person opening account.
8. Information on ID, such as signature, inconsistent with information on file at financial institution.
9. Application appearing forged or altered or destroyed and reassembled.
10. Information on ID not matching any address in the consumer report, Social Security number has not been issued or appears on the Social Security Administration's Death Master File, a file of information associated with Social Security numbers of those who are deceased.
11. Lack of correlation between Social Security number range and date of birth.
12. Personal identifying information associated with known fraud activity.
13. Suspicious addresses supplied, such as a mail drop or prison, or phone numbers associated with pagers or answering service.
14. Social Security number provided matching that submitted by another person opening an account or other customers.
15. An address or phone number matching that supplied by a large number of applicants.
16. The person opening the account unable to supply identifying information in response to notification that the application is incomplete.
17. Personal information inconsistent with information already on file at financial institution or creditor.
18. Person opening account or customer unable to correctly answer challenge questions.
19. Shortly after change of address, creditor receiving request for additional users of account.
20. Most of available credit used for cash advances, jewelry or electronics, plus customer fails to make first payment.
21. Drastic change in payment patterns, use of available credit or spending patterns.
22. An account that has been inactive for a lengthy time suddenly exhibiting unusual activity.
23. Mail sent to customer repeatedly returned as undeliverable despite ongoing transactions on active account.
24. Financial institution or creditor notified that customer is not receiving paper account statements.
25. Financial institution or creditor notified of unauthorized charges or transactions on customer's account.
26. Financial institution or creditor notified that it has opened a fraudulent account for a person engaged in identity theft.

*Source: Federal Trade Commission*

**Attachment 2**

*[Insert Physician Practice Name]*
**Identity Theft Prevention and Detection and Red Flag Rule Compliance Policy & Procedures**

## Policy

It is the policy of ***[physician practice name]*** to follow all federal and state laws and reporting requirements regarding identity theft. Specifically, this policy outlines how ***[physician practice name]*** will (1) identify, (2) detect and (3) respond to "red flags." A "red flag" as defined by this policy includes a pattern, practice, or specific account or record activity that indicates possible identity theft. It is the policy of ***[physician practice name]*** that this identity theft prevention and detection and Red Flags Rule compliance program is approved by ***[physician practice name Board of Directors or appropriate committee /representative]*** as of May 1, 2009, and that the policy is reviewed and approved no less than annually. It is the policy of ***[physician practice name]*** that ***[specific staff person's title here]*** is assigned the responsibility of implementing and maintaining the Red Flag Rule requirements. Furthermore, it is the policy of this ***[physician practice name]*** that this individual will be provided sufficient resources and authority to fulfill these responsibilities. At a minimum, it is the policy of ***[physician practice name]*** that there will be one individual or job description designated as the privacy official.

It is the policy of ***[physician practice name]*** that, pursuant to the existing HIPAA Security Rule, appropriate physical, administrative and technical safeguards will be in place to reasonably safeguard protected health information and sensitive information related to patient identity from any intentional or unintentional use or disclosure. It is the policy of ***[physician practice name]*** that its business associates must be contractually bound to protect sensitive patient information to the same degree as set forth in this policy. It is also the policy of ***[physician practice name]*** that business associates who violate their agreement will be dealt with first by an attempt to correct the problem, and if that fails by termination of the agreement and discontinuation of services by the business associate. It is the policy of ***[physician practice name]*** that all members of our workforce have been trained by the May 1, 2009, compliance date on the policies and procedures governing compliance with the Red Flag Rule.

It is also the policy of ***[physician practice name]*** that new members of our workforce receive training on these matters within a reasonable time after they have joined the workforce. It is the policy of ***[physician practice name]*** to provide training should any policy or procedure related to the Red Flag Rule materially change. This training will be provided within a reasonable time after the policy or procedure materially changes. Furthermore, it is the policy of ***[physician practice name]*** that training will be documented, indicating participants, date and subject matter.

## Procedures

### I. Identify Red Flags

In the course of caring for patients, ***[physician practice name]*** may encounter inconsistent or suspicious documents, information or activity that may signal identity theft. ***[physician practice name]*** identifies the following as potential red flags, and this policy includes procedures describing how to detect and respond to these red flags below:

1. A complaint or question from a patient based on the patient's receipt of:
    - A bill for another individual
    - A bill for a product or service that the patient denies receiving
    - A bill from a health care provider that the patient never patronized
    - A notice of insurance benefits (or explanation of benefits) for health care services never received
2. Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient.

3. A complaint or question from a patient about the receipt of a collection notice from a bill collector.
4. A patient or health insurer report that coverage for legitimate hospital stays is denied because insurance benefits have been depleted or a lifetime cap has been reached.
5. A complaint or question from a patient about information added to a credit report by a health care provider or health insurer.
6. A dispute of a bill by a patient who claims to be the victim of any type of identity theft.
7. A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.
8. A notice or inquiry from an insurance fraud investigator for a private health insurer or a law enforcement agency, including but not limited to a Medicare or Medicaid fraud agency.
9. ***[Insert other relevant practice-specific items here]***

**II. Detect Red Flags**

***[Physician practice name]*** practice staff will be alert for discrepancies in documents and patient information that suggest risk of identity theft or fraud. ***[Physician practice name]*** will verify patient identity, address and insurance coverage at the time of patient registration/check-in.

**Procedures:**

1. When a patient calls to request an appointment, the patient will be asked to bring the following at the time of the appointment:
    - Driver's license or other state issued photo ID
    - Current health insurance card
    - Utility bills or other correspondence showing current residence if the photo ID does not show the patient's current address. If the patient is a minor, the patient's parent or guardian should bring the information listed above.
2. When the patient arrives for the appointment, the patient will be asked to produce the information listed above. This requirement may be waived for patients who have visited the practice within the last six months. However, this is a minimal burden on the practice to require the information every visit.
3. If the patient has not completed the registration form within the last six months, registration staff will verify current information on file and, if appropriate, update the information.
4. Staff should be alert for the possibility of identity theft in the following situations:
    - The photograph on a driver's license or other photo ID submitted by the patient does not resemble the patient.
    - The patient submits a driver's license, insurance card, or other identifying information that appears to be altered or forged.
    - Information on one form of identification the patient submitted is inconsistent with information on another form of identification or with information already in the practice's records.
    - An address or telephone number is discovered to be incorrect, non-existent or fictitious.
    - The patient fails to provide identifying information or documents.
    - The patient's signature does not match a signature in the practice's records.
    - ***[If your practice collects Social Security number]***: The Social Security number or other identifying information the patient provided is the same as identifying information in the practice's records provided by another individual, or the Social Security number is invalid.

**III. Respond to Red Flags**

If an employee of ***[physician practice name]*** detects fraudulent activity or if a patient claims to be a victim of identity theft, ***[physician practice name]*** will respond to and investigate the situation. If the fraudulent activity involves protected health information (PHI) covered under the HIPAA security standards, ***[physician practice name]*** will also apply its existing HIPAA security policies and procedures

to the response. If potentially fraudulent activity (a red flag) is detected by an employee of ***[physician practice name]****:*

1. The employee should gather all documentation and report the incident to his or her immediate supervisor (or designated compliance officer/privacy official, if applicable).
2. The supervisor (or designated compliance officer/privacy official, if applicable) will determine whether the activity is fraudulent or authentic based upon the evidence presented.
3. If the activity is determined to be fraudulent, then ***[physician practice name]*** should take immediate action. Actions may include:

- Cancel the transaction
- Notify appropriate enforcement agencies
- Notify the affected patient
- Notify affected physician(s)
- Assess impact to practice.

If a patient claims to be a victim of identity theft:

- the patient should be encouraged to file a police report for identity theft if he/she has not done so already
- the patient should be encouraged to complete the ***ID Theft Affidavit*** developed by the FTC, along with supporting documentation **www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf**.
- ***[physician practice name]*** will compare the patient's documentation with personal information in the practice's records.

If following investigation, it appears that the patient has been a victim of identity theft, ***[physician practice name]*** will promptly consider what further remedial act/notifications may be needed under the circumstances, including:

- the physician shall review the affected patient's medical record to confirm whether documentation was made in the patient's medical record that resulted in inaccurate information in the record. If inaccuracies due to identity theft exist, a notation should be made in the record to indicate identity theft.
- the practice medical records staff will determine whether any other records and/or ancillary service providers are linked to inaccurate information. Any additional files containing information relevant to identity theft will be removed and appropriate action taken. The patient is responsible for contacting ancillary service providers.

If following investigation, it does not appear that the patient has been a victim of identity theft, ***[physician practice name]*** will take whatever action it deems appropriate.