AMA identity theft prevention and detection and Red Flags Rule compliance[1]: Sample policy

Please note: The information provided in this document does not constitute, and is no substitute for, legal or other professional advice. Seek consultation from legal or other professional advisors for individualized guidance regarding the application of the law to your particular situation or regarding other compliance-related concerns.

To customize this template document, replace the text in brackets (e.g., [text in brackets]) with text that is appropriate to your practice and circumstances. After customizing this document, it is advisable to have it reviewed by an attorney who is familiar with health privacy laws and regulations in the state(s) in which your practice is located and who is in a position to provide your practice with legal counsel.

To the extent possible, you should reword each section to reflect the specific procedures to be followed in your practice, and be sure to incorporate applicable state laws. In addition, you may decide that certain functions may only be performed by certain personnel, within certain departments or with a certain form of management approval. When appropriate, you may wish to include sanctions provisions. Sanctions are the disciplinary measures to be taken in the event of careless disregard or deliberate violation of any of these provisions. You may also wish to keep the documentation of sanctions in a separate sanctions policy.

[*Physician practice name*] Policies and procedures Identity theft prevention and detection and Red Flags Rule compliance

---

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.

[1] On December 18, 2010, the President signed into law the "Red Flag Program Clarification Act of 2010," which clarifies the type of "creditor" that must comply with the Red Flags Rule. The American Medical Association (AMA) is pleased that this law supports AMA's long-standing argument to the Federal Trade Commission (FTC) that the Red Flags Rule should not be applied to physicians generally. While the AMA believes that most physicians will not fall under creditor categories specified in the new law, the AMA has prepared a guidance document and this sample policy on identity theft prevention and detection for voluntary use.

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 June 1, 2010, and that the policy is reviewed and approved no less than annually.

It is the policy of [*physician practice name*] that [*specify title here*] is assigned the responsibility of implementing and maintaining the Red Flags 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 this [*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 June 1, 2010 compliance date on the policies and procedures governing compliance with the Red Flags 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 Flags 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; or
    - 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.

Procedure:

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 photo ID;
    - Current health insurance card; and
    - 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.**
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.

Procedure

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.
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 law enforcement;
    - Notify the affected patient;
    - Notify affected physician(s); and
    - Assess impact to practice.

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

1. The patient should be encouraged to file a police report for identity theft if he/she has not done so already.
2. The patient should be encouraged to complete the ID Theft Affidavit developed by the FTC, along with supporting documentation.
3. [*Physician practice name*] will compare the patient's documentation with personal information in the practice's records.
4. 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.
5. The physician will 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.
6. 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.
7. 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.