

2009 Red Flags Rule Policies and Procedures

NOTICE:

The following policies should be considered supplements to Chapter 15 of the MGMA *Operating Policies and Procedures Manual for Medical Practices, 3rd Edition*.

To obtain this manual, visit www.mgma.com/store and search for item 6495.

Medical Group Management Association® (MGMA®) publications are intended to provide current and accurate information and are designed to assist readers in becoming more familiar with the subject matter covered. Such publications are distributed with the understanding that MGMA does not render any legal, accounting, or other professional advice that may be construed as specifically applicable to an individual situation. No representations or warranties are made concerning the application of legal or other principles discussed by the authors to any specific factual situation, nor is any prediction made concerning how any particular judge, government official, or other person will interpret or apply such principles. Specific factual situations should be discussed with professional advisors.

Copyright © 2009 Medical Group Management Association

These policies were adapted with permission from the American Health Lawyers Association. 2009. All Rights Reserved.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the copyright owner.

Table of Contents

Policy 1511: General Identity Theft (“Red Flags”) Finance/Compliance Policy	3
Policy 1512: Recognize Identity Theft Red Flags	4
Policy 1513: Verify Patient Identity at Time of Registration/Check-in	5
Policy 1514: Investigate and Document Identity Theft	6
Policy 1515: Inform the Patient about Identity Theft.....	8
Policy 1516: Disposition of Medical Record when Identity Theft is Confirmed.....	11

Policy 1511: General Identity Theft (“Red Flags”) Finance/Compliance Policy

It is the policy of the Practice to implement an Identity Theft Prevention Program (the “Program”) to detect, prevent and mitigate identity theft in connection with new and existing patient accounts.

Policy:

To detect, prevent, and mitigate identity theft and enable the Practice to:

1. Identify relevant patterns, practices, and specific forms of activity that are “red flags” signaling possible identity theft and incorporate those red flags into our procedures;
2. Incorporate controls that detect red flags into our procedures;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Practice’s processes are updated periodically to reflect changes in risks from identity theft.

Definitions:

Identity theft is a fraud committed or attempted by using the identifying information of another person without authority. In the context of a medical practice, identity theft may involve using a person’s name and/or insurance information without his/her knowledge to fraudulently obtain medical services or benefits.

Policy 1512: Recognize Identity Theft Red Flags

It is the policy of the Practice to detect attempts at patient identity theft or fraud and immediately report incidents to the Administrator and his/her designee that occur in and/or around the Practice.

Procedures:

1. Staff should be alert for the possibility of patient identity theft.
2. Any staff member/witness suspecting identity theft should immediately report it to the Administrator.
3. The witness completes an identity theft investigation report.
4. The Administrator reviews the completed accident/incident investigation report.
5. If the Administrator determines it appropriate, the report is presented no later than at the next board meeting to determine the necessary follow-up with the party or parties involved.

In the following circumstances, staff should be vigilant in recognizing the possibility of identity theft:

- a. Upon check-in, the patient submits a driver's license, insurance card, or other identifying information that appears to be altered or forged.
- b. The photograph on the driver's license or other photo ID, as submitted by the patient, does not resemble the patient.
- c. The information on one form of the patient's identification is inconsistent with information on another form of identification (address on check for copayment does not match address on driver's license), or does not match information already in the Practice records.
- d. The patient Social Security Number (SSN) has not been issued; is listed on the Social Security Administration's Death Master File; or is otherwise invalid.

HINT: The following SSN numbers are **always invalid**:

- The first three digits are in the 800, 900, or 000 range;
 - The first three digits are in a range from 772 to 799;
 - The first three digits are 666;
 - The fourth and fifth digits are 00; or
 - The last four digits are 0000.
- e. The address given by the patient does not exist or is a post office box.
 - f. The phone number given by the patient is invalid or is associated with a pager or answering service.
 - g. The patient fails to provide identifying information or documents.
 - h. Personal identifying information given by the patient is not consistent with personal identifying information in the Practice's records.
 - i. The patient's signature does not match a signature on file in the Practice's records.
 - j. The SSN or other identifying information furnished by the patient is identical to other identifying information in the Practice's records as furnished by other patients.

Policy 1513: Verify Patient Identity at Time of Registration/Check-in

It is the policy of the Practice to verify patient identity at time of registration. The Practice will, to the extent feasible, request documentation of the patient's identity, residential address, and insurance coverage at time of registration as part of the Identity Theft Prevention Program.

Procedures:

1. When a patient calls to request or confirm an appointment, the patient will be asked to bring the following documentation at check-in for the appointment:
 - Driver's license or other government-issued photo ID; and
 - Current insurance card

NOTE: Be sure to tell the patient that if their photo ID does not show their current residential address (or if a P.O. Box is listed), then the patient should also bring a recent utility bill or other correspondence showing current residential address.

2. If the patient is a minor, the patient's parent or guardian should bring the information listed above.
3. When the patient arrives for the appointment, the patient will be asked to produce the information listed above. *NOTE: This requirement may be waived for patients who have been seen within the last six months.*
4. If the patient has not completed the registration form within the last six months, a new registration form must be completed upon registration or check in.

Policy 1514: Investigate and Document Identity Theft

It is the policy of the Practice to immediately investigate potential identity theft or fraud, especially in circumstances where a patient claims to be the victim of identity theft.

It is the policy of the Practice to report these incidents to the Administrator and his/her designee immediately.

Procedures:

If a patient claims to be a victim of identity theft, the Practice or its collection agency will investigate the claim. The patient must have previously filed a police report for identity theft, and the patient must complete one of the following three documents:

1. The ID Theft Affidavit developed by the FTC, including supporting documentation;
2. An ID theft affidavit recognized under state law; or
3. A written statement that includes the following documentation:
 - a. A statement that the patient's is a victim of identity theft;
 - b. A photocopy of the patient's driver's license or government-issued photo identification card;
 - c. Any other identification document that supports the statement of identity theft;
 - d. Specific facts supporting the claim of identity theft, if available;
 - e. Any other explanation that the patient did not incur the debt;
 - f. Any available correspondence disputing the debt;
 - g. Documentation of the residence of the patient at the date of service, including copies of utility bills, tax statements, or other statements from businesses sent to the patient at his or her residence;
 - h. A telephone number for contacting the patient;
 - i. Any information that the patient may have concerning the person who registered in his or her name;
 - j. A statement that the patient did not authorize the use of his or her name or personal information for obtaining services; or
 - k. A statement certifying that the representations are true, correct, and contain no material omissions of fact to the best knowledge and belief of the person submitting the certification.

In addition, the patient must cooperate with comparing his or her personal information with information in the Practice's records.

If following investigation, it appears that the patient has been a victim of identity theft; the Practice will take the following actions:

1. The Practice will cease collection on open accounts that resulted from identity theft. If the accounts had been referred to collection agencies or attorneys, the collection agencies/attorneys will be instructed to cease collection activity.
2. The Practice will cooperate with any law enforcement investigation relating to the identity theft.
3. If an insurance company, government program or other payer has made payment on the account, the Practice will notify the payer and refund the amount paid.
4. If an adverse report had been made to a consumer reporting agency, the Practice will notify the agency that the account was not the responsibility of the patient.

If following investigation, it does not appear that the patient has been a victim of identity theft, the Practice or the collection agency will give written notice to the patient that he or she is responsible for payment of the bill. The notice will state the basis for determining that the person claiming to be a victim of identity theft was, in fact, the patient.

Policy 1515: Inform the Patient about Identity Theft

It is the policy of the Practice to immediately inform the patient – in writing – of possible unauthorized use of their personal identifying information.

Notice shall only be delayed if law enforcement informs the Practice that disclosure of the identity theft or breach would impede a criminal investigation or jeopardize national security. A request for delayed notification must be made in writing (or documented contemporaneously by the Practice in writing), including the name of the law enforcement officer making the request and the officer’s agency engaged in the investigation.

The required notice shall be provided without unreasonable delay after the law enforcement agency communicates to the entity its determination that notice will no longer impede the investigation or jeopardize national or homeland security.

Procedure:

A formal letter will be mailed to the patient via certified USPS mail, return receipt requested. The letter will state the reason the Practice feels the patient is a victim of identity theft and the recommended steps the patient should undertake.



Sample Letter to Patient

[Date]
Sent by CERTIFIED MAIL, RETURN RECEIPT REQUESTED

[Patient Name]
[Patient Address]
[Patient City, State, ZIP]

Re: Suspected Identity Theft

Dear [Patient Name]:

This letter addresses the unauthorized use of your name and other personal information at [Practice name] on [date]. [Explain factual situation and describe compromise of information in detail (e.g. how it happened, information disclosed, what actions have been taken to remedy situation, etc.)].

We have reported this incident to [law enforcement officer’s name] at the [local law enforcement agency], who can be reached at [phone or email contact]. We also have placed an alert on your account at this facility in an effort to prevent further misuse of your identity.

Medical identity theft is very serious because, in addition to causing financial problems, identity theft can lead to inappropriate medical care when incorrect information is included in a patient’s medical record. If you believe you are the victim of medical identity theft, you should ask to review and make appropriate corrections to your medical record so that you receive appropriate care.

For your health and safety, it is very important that your medical records do not contain information about another person. **We request your assistance in ensuring that our records about you are correct.**

We have removed from your medical record information relating to care given on [date] because [we/you] have indicated you did not receive services at this office on those dates. After removing that information, your medical record shows the following visits:

Date of Visit: _____

Reason for visit: _____

If you do not remember one or more of these visits, please contact us immediately. You can review your entire medical record by visiting this office, and we encourage you to do so. In addition to making sure your medical record with this facility is accurate, we encourage you to check the accuracy of your records with other health care providers and your health insurance plan(s).

Based on the information we have received related to the improper use of your name and other identifying information on [date], this office will not bill you or your insurer for the services it provided at that time. We are in the process of correcting your account with your health insurer. We recommend that you carefully monitor explanations of benefits (EOBs) received from your health insurer to determine if any other person has used your identity to obtain health care. If you receive an EOB or bill for health care you do not remember obtaining, immediately contact your insurer and the health care provider who furnished the services.

We recommend that you place a fraud alert of your credit file immediately. A fraud alert tells creditors to contact you and verify your identity before they open any new accounts or change existing accounts. Please contact one of the three major credit bureaus. Once a credit bureau confirms your fraud alert, the others are also notified to place fraud alerts.

- **Equifax**, P.O. Box 740241, Atlanta GA 30374-0241, www.equifax.com, 1-800-525-6285
- **Experian**, P.O. Box 9534, Allen, TX 75013, www.experian.com, 1-888-EXPERIAN
- **Trans Union**, Fraud Victim Assistance Division, P.O. Box 6790, Fullerton CA 92834-6790, www.transunion.com, 1-800-680-7289

When you receive a copy of your credit report(s), review it carefully and continue monitoring your credit reports to be certain there have been no unauthorized transactions made or opened in your name. Look for inquiries from creditors that you did not initiate. Also review your personal information for inaccuracies, such as prior addresses and wrong social security numbers.

If you see anything you do not understand, call the credit reporting agency at the telephone number listed on the report.

Under federal law, you are entitled to receive one free comprehensive disclosure/report of all the information in your credit file from each of the three national credit bureaus listed above once every 12 months. You may request a free annual credit report by visiting the websites noted above. Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every three months for the next year.

If you find suspicious activity of your credit reports or have reason to believe your information is being misused, immediately notify the credit bureaus.

If you believe an unauthorized account has been opened in your name, immediately contact the financial institution that holds the account.

You should also file a police of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records. Creditors want the information it contains to absolve you of the fraudulent debts.

You should also file a complaint with the FTC at www.ftc.gov/idtheft/ or 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement agencies for their investigations.

We encourage you to report any helpful information to [investigating law enforcement officer] at the [local law enforcement agency]. We also encourage you to alert area hospitals and other health care providers that your identifying information is being used in a fraudulent manner.

If there is anything this practice can do to assist you, please call our [Compliance Office/Privacy Officer] at [telephone number].

Sincerely,

[Administrator/Title]

[Practice name]

Policy 1516: Disposition of Medical Record when Identity Theft is Confirmed

It is the policy of the Practice to immediately isolate and correct errors in a patient medical record(s) resulting from identity theft.

Procedures:

1. If it is confirmed that a patient record was created or modified as the result of identity theft, a notation concerning the identity theft will be placed in the record.
2. All demographic information will be removed from the record.
3. Medical records staff will determine whether any other records are linked to the record found to be created through identity theft.
4. In some cases, identity theft may involve an identity thief receiving care under the name of another person, who also has been a patient. In such a case, other files relating to the patient will be reviewed and any information relating to the identity theft will be segregated and removed.