



Guidance for Psychologists on “Red Flag Rules” Compliance

By Legal and Regulatory Affairs Staff

July 31, 2009 Update: The Red Flags Rule is now scheduled to take effect on November 1, 2009.

March 26, 2009 – The “Red Flag Rules” (Rules) from the Federal Trade Commission (FTC) take effect on May 1, 2009. Some psychologists may need to comply with the rules, which are intended to reduce identity theft. This article and appendices offer guidance for practitioners.

“Red flags” is a term the FTC uses to refer to “potential patterns, practices or specific activities indicating the possibility of identity theft.” Although the agency has stated that the Rules were designed primarily for financial institutions and other traditional creditors, the FTC announced last fall that that it would also apply the Rules to health care practitioners who are considered “creditors.”

Health care practitioners are considered “creditors” if they:

1. Provide services and then bill patients later; **or**
2. Regularly allow their patients to defer payment for services -- including by setting up payment plans -- on a “regular” basis.

If you meet either of these criteria, the Rules will apply to you.

We contacted the FTC to determine how often a psychologist would have to permit delayed payment for that practice to be considered “regular” under the second situation noted above. Based on informal guidance from the agency, we recommend that you should expect that second situation applies to you **unless** you only let patients defer payment on a rare or sporadic occurrence, and when your normal payment policies do not provide for patients to defer payments. When these circumstances exist, the practice of extending credit probably would not be considered “regular.” By contrast, if you allow your clients to delay payment more often than on a rare or sporadic basis, you should plan to comply with the Rules.

The FTC believes that the Rules are important in the health care industry because of the rising incidence of identity theft related to medical information. Medical identity theft involves using someone else’s personally identifiable information — such as name, date of birth, social security number or insurance policy number — to bill for goods and services related to health care. These acts can seriously damage the victim’s medical record and credit. They can also lead to inappropriate care if health care providers rely on the inaccurate information in the victim’s medical record to make health care decisions.

Egregious examples of medical identity theft include a man receiving \$350,000 in cardiac surgery services using a neighbor’s identity. Another victim, whose identity was stolen by a person seeking to obtain surgery, discovered that the identity thief’s medical information was commingled with her own when she found an incorrect notation of diabetes in her record.

What to do if the rules apply to you

If the Red Flag Rules apply to you, you must develop and implement a written “identity theft prevention program” (Program) ~~designed to identify, detect and respond to suspicious activities~~ (Red Flags) that could indicate that identity theft is happening in your practice. As reiterated in new compliance guidance that the FTC issued on March 23, 2009 (available at <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf>), the Program can be tailored to the size and risks of your practice. For solo or small group practices, the Program can consist of simple written policies.



To assist you with compliance, Attachment A is a Sample Red Flag Program designed for solo and small group practitioners. Practitioners in larger group practices or organizational settings should be guided by the organization's Red Flags policies.

Your Program should:

- Include a policy governing how your practice will verify patient identity at the time of intake, specifying what documents will be used for identification and what information will be requested.
- Have a policy stating that the staff person who takes the intake information should also be alert for conflicting information, for example, a discrepancy in identifying information such as address or age.
- Specify how you will respond if a Red Flag is detected. Responses may include contacting the patient if necessary, changing passwords to patient accounts or notifying law enforcement.
- Provide for appropriately and effectively managing "service providers." These appear to be the equivalent of and serve the same purpose as "business associates" under the Health Insurance Portability and Accountability Act (HIPAA). (A "business associate" is an organization or person other than a member of the psychologist's workforce who receives patient information from the psychologist to provide services to, or on behalf of, the psychologist – for example, accountant, lawyer, billing service or collection agency.) Because the term "business associate" is more familiar to psychologists and better defined than "service providers," we use the former term. Attachment B to this article contains a sample program that you can add to your existing business associates contracts, if you have them, or that you can have your service providers sign as a standalone agreement.
- Require that you review the Program annually to ensure its effectiveness.

An appendix to the FTC Rules gives examples of Red Flags that your practice may encounter, such as suspicious documents (for example, a driver's license that appears to be forged or tampered with) and questionable personal information (a changed address when the patient has made no mention of moving). We have incorporated into our Sample Program (Attachment A to this article) those red flags that we believe are most likely to apply to a solo or small group psychology practice.

Some practitioners may wonder whether complying with the HIPAA Security Rule will obviate compliance with the Red Flag Rules. The answer is "no." Following best security practices, such as those identified in the Security Rule for electronic patient information as well as in the [2007 APA Record Keeping Guidelines http://www.apapractice.org/apo/insider/professional/apaapproved/revise_d_apa_record.GenericArticle.Single.articleLink.GenericArticle.Single.file.tmp/Record%20Keeping%20Guidelines%202007.pdf](http://www.apapractice.org/apo/insider/professional/apaapproved/revise_d_apa_record.GenericArticle.Single.articleLink.GenericArticle.Single.file.tmp/Record%20Keeping%20Guidelines%202007.pdf) should help to lower your risk of identity theft. But it will not preclude your having to comply with the Red Flag Rules.

The FTC is charged with enforcing the Red Flag Rules. Failure to comply may result in penalties of up to \$2,500 per violation.

The APA Practice Organization will keep you informed as the FTC makes available additional guidance and information regarding the Rules and how they apply to psychologists.

PLEASE NOTE: Legal issues are complex and highly fact-specific and require legal expertise that cannot be provided by any single article. In addition, laws change over time and vary by jurisdiction. The information in this article should not be used as a substitute for obtaining personal legal advice and consultation prior to making decisions regarding individual circumstances.



Attachment A

Sample Program for Compliance with “Red Flag Rules” Regarding Identity Theft

The following Identify Theft policies are hereby adopted by the [insert name or title of key decision makers, for example, management, Board of Directors] of [insert the name of your practice] (the Practice):

In this program, “Staff” refers to the Practice’s workforce members (including non-paid staff such as interns and volunteers) who are **not** psychologists or mental health professionals (Practitioners). However, if the Practice only has Practitioners, they will perform the Staff duties in Section A.

A. Staff will ask patients to provide identification at the first session.

1. Staff will request documentation of identity and make copies of the documentation provided:

- Driver’s license, passport or other government issued photo ID.
- If the photo ID does not have the current address, Staff will request a utility bill, lease or other evidence of current address.
- Current insurance, Medicare or Medicaid card (for patients relying on such reimbursement).

2. Staff will verify that the ID photo looks like the patient and that other descriptions in the ID, like height and weight, appear to be correct.

3. Copies of this information shall be kept in the patient’s file or in another secure location.

B. Practitioners and Staff shall be alert to and act on evidence of fraud.

Staff shall be alert to suspicious activity such as:

- Identification documents that appear altered or forged
- Information provided by client is inconsistent e.g., information on one form of identification submitted is different from information on another form of identification (such as age, address, occupation)
- Suspicious change of address notice (for example a move from an expensive to an inexpensive neighborhood)



- Evidence that your paper or electronic records may have been compromised, for example, you discover that a Staff member accessed patient files without authorization, or that locked patient files have been broken into.

2. Staff shall act upon suspicious activities or evidence of identity theft as

appropriate by:

- Checking with other members of the Practice regarding suspicious events, for example, if Staff receives a suspicious change of address notice (see B1c.), Staff will ask the practitioner treating that patient to consider whether such a change is consistent with information the patient has reported in psychotherapy.
- Contacting the patient to verify suspicious information
- If there is still a suspicion of identify theft after taking the verification steps above, contacting local law enforcement after obtaining patient permission.
- Changing passwords on electronic record accounts that may have been compromised
- Notifying patients where it appears that they may have been victims of identity theft.

C. The Practice will respond to reports of identity theft.

The Practice will respond to reports of actual or suspected identity theft by patients, law enforcement, and others as appropriate, including by identifying the situations listed in B2.

D. The Practice will ensure that staff and Practitioners are trained on implementing the policies.

1. Staff and Practitioners will be trained in the implementation of these policies
2. Staff and Practitioners will be given a copy of this policy to read and initial.

E. The Practice will have business associates sign Red Flag Agreements.

The Practice will determine whether it has business associates who handle patient information, e.g., billing services, collection agencies, accountants. It will ask those business associates to do one of the following:



- Sign an addendum to the business associates contract that the Practice already has in place with that company as part of HIPAA Privacy Rule/Security Rule compliance; or if no business associates contract is in place,
- Sign a standalone agreement, or
- Provide a copy of its own Red Flags Program and state that such Program meets the requirements of the Red Flags Rules.

See Attachment B for a model agreement designed to the first two bullets above.

F. The Practice will re-evaluate these policies periodically.

The Practice will annually re-evaluate whether these policies are effective and appropriate for detecting and preventing identity theft in light of the Practice's actual experience with actual or suspected identity theft and in light of any new information learned by the Practice regarding identity theft risks.

Date of Adoption of policies: _____

PLEASE NOTE: Legal issues are complex and highly fact-specific and require legal expertise that cannot be provided by any single document. In addition, laws change over time and vary by jurisdiction. The information in this document should not be used as a substitute for obtaining personal legal advice and consultation prior to making decisions regarding individual circumstances.



Attachment B

Instructions:

This document is for use with any business associates who handle patient information as described in the March, 26, 2009 *PracticeUpdate* e-newsletter article on the Red Flag Rules and as described in Section E of the Sample Red Flag Program (Attachment A to the article).

If you do not have an existing business associate contract with such entities, use Title and Intro A. If you do have a business associate contract, use Title and Intro B. Please use only one of the options and delete the option that you do not use on your signed document.

Title and Intro A

Sample Red Flag Agreement for Business Associates

This Agreement is made between [name of psychology practice] (Practice) and [name of bus assoc] (Business Associate). The parties are agreeing to take such action as is necessary to comply with the requirements of the Red Flags Rules. The purpose of this Agreement is to make the Practice compliant with the requirements of the Red Flag Rules (12 CFR Section 681.2, (b)(10) and (e)(4)) that the Practice ensure that the activities of the Business Associate will be conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

Title and Intro B

Sample Addendum to Business Associates Contract

This is an Addendum to the Business Associates Contract is made between [Name of psychology practice] (Practice) and [Name of business associate] (Business Associate) dated [insert date of original Business Associate Contract]. The Parties are agreeing to take such action as is necessary to comply with the requirements of the Red Flag Rules (12 CFR 681). The purpose of this Addendum is to make the Practice compliant with the Red Flag Rules requirements (12 CFR Section 681.2, (b)(10) and (e)(4)) that the Practice have in place a Business Associate contract that will ensure that the activities of the Business Associate will be conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

A. Business Associate shall be alert to and act on evidence of fraud.

Business Associate shall be alert to suspicious activity such as:



- Identification documents that appear altered or forged
- Information provided by client is inconsistent, for example, information on one form of identification submitted is different from information on another form of identification (such as age, address, occupation)
- Suspicious change of address notice (for example a move from an expensive to an inexpensive neighborhood)
- Evidence that your paper or electronic records may have been compromised, for example, you discover that a Staff member accessed patient files without authorization, or that locked patient files have been broken into

Business Associate shall act upon suspicious activities or evidence of identity theft as appropriate by notifying Practice as follows:

- Notifying the Practice of suspicious activity
- Investigating any suspicious activity that may have occurred within Business Associate's operation, for example, unauthorized access by Business Associate's employees.
- Taking corrective action to the extent that suspicious activity appears to have occurred within Business Associate's operation
- Changing passwords on electronic record accounts that may have been compromised
- Notifying Practice where it appears that Practice or its patients may have been victims of identity theft



B. Business Associate will ensure that its staff is trained on implementing this agreement/addendum.

1. Business Associate's management and employees will be trained in the implementation of these policies.
2. Business Associate's management and employees will be given a copy of this policy to read and initial.

BUSINESS ASSOCIATE:

PRACTICE:

Signature

Signature

Print Name and Title

Print Name and Title

Date

Date

PLEASE NOTE: Legal issues are complex and highly fact-specific and require legal expertise that cannot be provided by any single document. In addition, laws change over time and vary by jurisdiction. The information in this document should not be used as a substitute for obtaining personal legal advice and consultation prior to making decisions regarding individual circumstances.

UPDATED July 31, 2009