

NDA MEMO: ATTENTION NDA MEMBERS!!

April 1, 2009

A New FTC Rule is Scheduled to go into Effect Aug. 1, 2009

Important That You Read This - Sample Policy Attached

ADA GUIDANCE FOR COMPLIANCE WITH THE NEW FTC "RED FLAGS" RULE

Despite all the talk about "identity theft" it remains a growing problem. As you know, it has been the subject of many news stories over the past few years that recount the experiences of people who have done nothing wrong themselves, but whose credit cards, social security numbers, and other identifying information have been used by criminals to ring up huge debts, causing serious financial and legal problems for the victims. To fight this problem, the Federal Trade Commission (FTC) has issued regulations requiring any business that may provide credit to customers to take certain steps to guard against identity theft. The FTC has taken the position that its "Red Flags Rule" extends to health care providers, including dentists. **The new FTC rule is scheduled to go into effect on Aug. 1, 2009.**

This guide provides a step-by-step plan to help prepare and implement the requirements of the Rule. A sample identity theft policy and procedures program is attached as Appendix A. Beware! There are many software vendors and seminar providers attempting to capitalize on health care providers' memories concerning the complexities associated with HIPAA when it was implemented. Seminars and software products costing hundreds, even thousands, of dollars have been hawked to dental and other healthcare practices. Whether you wish to purchase any of these products or services is, of course, completely up to you, but is probably not necessary.

ADA legal staff has been closely following the development of the FTC's position on the Red Flags Rule as they apply to dentists and other health care providers. On November 24, 2008, the ADA's Chief Legal Counsel sent a letter to the FTC explaining the major legal arguments against applying the Red Flags Rule to dental offices. Similar complaints had been lodged with the FTC in communications sent by other health care provider associations, and these arguments resulted in the FTC postponing enforcement of the Rules with respect to dentists and physicians from November 1, 2008 to the current August 1 date.

On Wednesday, March 4, 2009, ADA legal staff, ADA President Dr. John Findley, and outside counsel conducted a telephone conference lasting more than an hour with FTC staff. The ADA representatives explained all of the practical reasons why the Red Flags Rule should not be applied to dental practices. For example, Dr. Findley recounted that he had never had an identity theft problem in his own practice of thirty-eight years, and that in speaking to dentists across the country as ADA President Elect and President he had never heard the issue raised by any of the thousands of dentists he has spoken to. Dr. Findley pointed out that more than 63% of all dentists maintain sole practices and that fully 83% of all dentists are in practices comprising no more than two dentists. He said that enforcing Red Flags programs in the vast majority of practices where they are not needed would place a financial burden on dentists who are already feeling the effects of the bad economy and also interfere with the personalized, trusting doctor patient relationship that dental offices seek to foster.

The FTC staff explains that: Health care providers can be the first to spot the red flags that signal the risk of identity theft, including suspicious activity indicating that identity thieves may be using stolen information

like names, Social Security numbers, insurance information, account numbers and birth dates to open new accounts or get medical services.

The FTC's extension of the compliance deadline only applied to the part of the Rules requiring an identity theft detection and response plan. Dental offices that utilize consumer credit reports should already be complying with another provision of the Rules that requires correction of address discrepancies in consumer credit reports. FTC staff members replied that the Red Flags Rule were intended to be "very flexible" and that a Red Flags plan need only address those circumstances that a dental practice actually encounters. One staff member went so far as saying that if a dental practice has not experienced Red Flags situations in the past, a program that simply directs dental office team members to be aware of the problem of identity theft generally and to report particular occurrences that make them suspicious will satisfy the Rule.

FTC staff also represented that they were working on written guidance to address the sort of "low risk" environments into which they conceded most dental practices appear to fall. The ADA representatives asked when the new guidance would issue, to which the FTC replied, "hopefully soon." The ADA then pointed out that as a practical matter the deadline for adopting Red Flag plans should be postponed until after the guidance was released. FTC staff responded that they were not in a position to make that decision, but they would speak to their supervisors on the subject.

What is a "Red Flag"? - A red flag is some event, document, information, or attempted transaction that should alert the business or healthcare practice that someone is not who he or she claims to be - in other words, an indication of a possible identity theft.

As stated above, many dental practices may only rarely, or even never, encounter Red Flags or identity theft situations, but in the context of a dental practice red flags might include: 1. An individual falsely claiming to be someone else known to the office staff; 2. An unrecognized individual with no personal identification or who refuses to provide information about their identity; 3. An individual who is unable or unwilling to provide contact information; 4. Suspicious documents that appear to have been altered or that contain information that does not match the person presenting them; 5. Altered or cancelled insurance cards; 6. Attempts to submit by phone a patient's credit card or insurance information as payment for services; 7. Any form of notice stating that a patient's information or identity may have been stolen; 8. A notice that the patient is on active duty in the armed forces; 9. Addresses discrepancies in consumer credit reports; 10. Disputes about bills by a patient claiming to be a victim of identity theft; 11. Undeliverable mail or returned checks; 12. Suspicious requests for a prescription or a refill; 13. Any other suspicious activity in relation to patient accounts, including evidence of security breaches (e.g., theft of a computer containing patient information), and unusual activity in relation to such account; and, 14. Discrepancies between the patient's purported medical records and the patient's physical condition.

Why Dental Offices May Be Covered by the Rules - According to the FTC a dental office is covered by the Red Flags Rule if it is considered a "creditor" and it has at least one "covered account."

When Does a Dental Practice Qualify as a Creditor? - The Rule defines a "creditor" very broadly. Examples of instances where a dental office will be considered a creditor under the Rules include where the practice: (a) sends a bill to a patient for services rendered; (b) agrees with the patient on an installment payment plan; (c) arranges for the patient to obtain credit to pay for services through a medical financing company such as CareCredit®; and (d) accepts insurance where the patient is ultimately responsible for payment. In practice, it seems that the only dental offices that will not be considered creditors are those that always require payment at the time dental service is provided. Although coverage is very broad, it does not appear that accepting payment by credit card alone qualifies an organization as a creditor.

What Accounts in a Dental Office Are So-Called “Covered Accounts”? - A patient account is a “covered account” if it contains information that may place the patient or the dental practice at a “reasonably foreseeable risk” of harm from identity theft. Patient account files meet this definition because they contain identifying patient information such as names, addresses, dates of birth, emergency contacts, and banking and insurance information, for use in connection with subsequent patient visits. Prescription information can also present a risk of identity theft.

Complying with the Rules - To comply with the Rules, a dental office must adopt a written policy and procedures designed to: 1) identify Red Flags relevant to the practice; 2) explain how Red Flags will be detected; 3) describe procedures to respond to any detected Red Flags; and 4) establish procedures to administer the program, including training and periodic review and evaluation of the program. The step-by-step procedures described below, and the sample Identity Theft Detection and Response Policy and Procedures attached as Appendix A will help dental offices prepare and implement a Red Flags program appropriate for their particular practices. The following recommended steps are based on the statements the FTC staff made during the March 4, telephone conference and, as such, are less detailed and hopefully are less burdensome than the procedures that appear to be required by the published Red Flag regulations.

Step One: Identifying Red Flags - Along with every other organization subject to the Red Flags Rule, a dental practice’s Red Flags program should create a list of potential Red Flags indicators that are relevant to the particular practice based on its past experience. In considering this issue, a dental practice may find it helpful to consult the list in the “What is a Red Flag?” section above, along with examples from its own experience. When establishing detection procedures, be aware that some other types of identification can themselves lead to an increased risk of identity theft. For example, unless used as an insurance identification number or is otherwise necessary, a dental practice should consider not requesting Social Security Numbers from patients.

Step Two: Detecting and Addressing Red Flags - Once the relevant Red Flags have been identified, the next step is to establish written procedures to address them. Each office will need to determine how far it will go in establishing formal procedures. The program’s procedures for addressing Red Flags, if and when they arise, may include: Contacting the patient to verify or report information. Monitoring patient accounts to verify identity at a later date. Refusing to provide services to an individual in a potential identity theft situation unless professional ethics dictate otherwise. Notifying the authorities. Concluding that no action is necessary.

A non-exhaustive list of some possible situations a dental office might face and possible responses to them might include: A person falsely claims to be a patient or other person known to the office. An appropriate response would be to refuse to provide services to the imposter and notify the person whose identity has been taken. A suspicious person cannot provide identification and has a “friend” call on the telephone with a credit card number for payment. Here, since the person is expressly seeking credit, an appropriate response would be to advise the person that services cannot be provided on that basis. A patient’s bill is returned as undeliverable at the address provided. An appropriate response would be to investigate by making sure the bill was sent to the address on file and by calling the patient to verify the address.

Two of the potential Red Flags identified by the FTC require specific responses, which the written program must include. First, if the dental office has obtained a consumer credit report for a patient that contains a discrepancy between the address provided by the patient and the address contained in the credit report, the dental office must make a reasonable attempt to verify the correct address. If the address that is verified is different from the address in the credit report, the practice must report this to the credit agency. Second, if

the dental office receives notice of an actual identity theft relating to one of its patient accounts, it must immediately cease any collection efforts against the alleged victim of the theft.

There may be related legal requirements for dental offices that utilize credit reports, including prohibitions against providing credit to patients who have consumer fraud alerts or active duty reports in credit reports. When responding to Red Flags keep in mind that other laws may impose legal obligations on the practice, such as HIPAA's patient privacy protections, and professional ethics considerations. The practice should consult with its own attorney where specific legal questions arise.

Step Three: Formalizing and Administering the Red Flags Program - Program Management -

The practice owner or leader is responsible for implementing and administering the program. An office manager or other staff member can be delegated as the Program Administrator so long as the practice leader retains and exercises oversight and approval of the program. The Program Administrator should be notified when any Red Flags are detected and oversee the appropriate response. A log describing and documenting responses to detected Red Flags should be kept.

Training - All staff should be trained to carry out the practice's Red Flags Rule program. The training program should cover the topics in this guide as tailored for the needs and experience of the particular practice. It should explain the purpose of the program, the relevant Red Flags and the procedures for responding to them. Training should be conducted during normal business hours. All staff should be given a copy of the program document, and should sign a written acknowledgement that they have read it and been given the opportunity to ask questions about it. Keep copies of these acknowledgements in the office administrative files.

Review and Evaluation - The Red Flags Rule require periodic review and evaluation of the practice's program by management. Review the program and Red Flags log at least annually to determine whether any modifications are needed; more frequently if incidents occur that suggest a need for modification.

Arrangements with Service Providers - According to the FTC regulations, a Red Flags Rule program must "exercise appropriate and effective oversight of service provider arrangements." In the case of dental practices such service provider arrangements might include agreements with credit card companies, other credit organizations, and dental labs. In order to "exercise appropriate and effective oversight," the practice should check its agreements with these providers to see if they positively state that they guard against identity theft and, if not, either check further to confirm that a provider has protections against identity theft or decline to enter into an agreement with that provider.

The program's effectiveness can be enhanced by educating patients about the practice's identity theft mitigation policy and procedures. Post in your reception area a notice advising that photo identification may be requested and a copy of the identity theft detection and prevention policy and procedures. Remind patients to bring any required documents to the office for their visit.

Penalties for Non Compliance - There are no criminal penalties for failing to comply with the Red Flags Rule, but dentists who are subject to the Rule and are found to have violated them may be subject to civil monetary penalties of up to \$2,500 per violation. Statements by FTC staff suggest that, at least initially, the FTC will rely on good faith implementation and will not be checking dental practices to make sure they have developed a program. Comments by FTC staff, however, are subject to change and are not binding on the agency.

Final Comments - While this guide attempts to provide dentists with the tools needed to comply with the Red Flags Rule, it has not been approved by the Federal Trade Commission (“FTC”) nor should it be treated as legal advice. With the wide range of differences among dental offices, practices should adapt these suggestions to meet the unique circumstances they encounter. We will provide updates as new information becomes available and, of course, dental practices should obtain legal advice on specific legal matters from their own attorneys.

The ADA’s Estimate of Red Flags Rule Compliance Costs for Dentists

The ADA estimates that the cost to implement and manage a Red Flags Rule (the “Rule”) program could exceed \$600 for the average dentist. Based on the fact that there are approximately 130,000 dental offices in the U.S., the aggregate cost to dentistry (and ultimately consumers) would be approximately \$79 million.

Prepared by the American Dental Association
Received by NDA, 3/29/09

APPENDIX A

Sample Identity Theft Detection And Response Policy and Procedures

IMPORTANT NOTE: While this model Policy attempts to provide dentists with the tools needed to comply with the Red Flag Rules, it has not been approved by the Federal Trade Commission (“FTC”). It should not be treated or considered as legal advice or as applicable to each dental practice. Rather, each practice should adapt this model Policy in light of its own experience and the advice that it receives from its counsel. The ADA and NDA will provide updates as new information becomes available. Mahalo.

I. Policy

This office has adopted an Identity Theft Detection and Response Policy and Procedures Program (“Program”) pursuant to the Federal Trade Commission's Red Flag Rules (“Rules”). The purpose of the Program is to assist in detecting, preventing, and mitigating instances of possible identity theft in connection with patients in our practice. It does so by (a) requiring us to verify the identity of all new patients, (b) establishing certain “Red Flags” that could indicate possible identity theft, and (c) requiring follow up on any incident which triggers a Red Flag. The Program must be observed by all employees of this practice, including the professional, administrative, and clerical staff,

II. Red Flags that May Indicate Identity Theft

1. An individual falsely claiming to be someone else who is known to the office staff;
2. Unexplained discrepancies between the patient’s medical records and the patient’s physical condition.
3. A discrepancy between the address contained in the patient’s consumer credit report and the address provided by the patient; [include this in your program only if the practice obtains credit reports in connection with providing patient services]
4. A report by a patient known to the office staff that he or she has been the victim of identity theft in connection with oral health care services provided by the practice;

III. Responding to Red Flags

Any employee of this practice who encounters a Red Flag situation or any other activity that may indicate identity theft should report the situation to _____. That person will follow up as appropriate and will record the incident and its handling in a Red Flags Log kept in this office. **Possible responses to a Red Flag situation include the following:**

a. Patient notification

The practice may notify the patient if a Red Flag is encountered that involves that patient’s identity. Notification may be provided by mail, by telephone, or in-person – as the practice deems appropriate. The notification may include verification that the patient has not been victimized by identity theft in connection with any visits to the practice.

In some instances, additional specific action will be required:

- If notice of an actual identity theft is received, we will immediately cease any collection efforts that are related to the identity theft.
- If a consumer credit report contains an address different from the address provided by the patient, the correct address will be verified with the patient. If the verified address is different from the address in the credit report, we may report the verified address to the credit reporting agency.

b. Notification of Legal Authorities

If the practice obtains specific information pertaining to a person committing identity theft, we will provide that information to law enforcement to the extent permitted under HIPAA and other privacy rules. We may seek advice of legal counsel on the issues involved.

Of course, if a Red Flag is triggered but we determine that there clearly has been no identity theft, no action will be taken.

IV. Plan Administration and Updates

All employees of this practice will receive a copy of this Policy and will be instructed as to its procedures. We will ask each employee to sign an acknowledgement of receipt and understanding. We will evaluate our Program annually and update it in light of experience. Any questions about this Policy should be addressed to _____.

ACKNOWLEDGEMENT (to be completed by all staff members who interact with patients)

I, _____, have read the practice’s Identity Theft Detection and Response Policy and Procedures and understand the contents. I have been instructed regarding situations that may suggest possible identity theft as described in the Identity Theft Detection and Response Policy and Procedures. If I discover a possible instance of identity theft, I will immediately bring the matter to the attention _____.

Approved by: _____
 Staff Name: _____ Staff Signature _____
 Title: _____
 Effective date: _____
 Review date: _____