

# Legal Q/A

---

Bruce E. Wood, Esquire

**Q:** *Does my practice need to comply with the FTC Red Flags Rule?*

**A:** Not today, but maybe on August 1.

On April 30 the Federal Trade Commission ("FTC") announced that it was delaying the enforcement of the Red Flags Rule, originally scheduled for November 1, 2008 and later extended to May 1, 2009, to August 1, 2009. The Red Flags Rule imposes obligations on "creditors" – including physicians – to detect, prevent and mitigate identity theft. The AMA and other medical organizations have aggressively tried to persuade the FTC that physicians are not "creditors" and should not be subject to the Red Flags Rule. So far, the FTC has stood firm noting that the consequences of medical identity theft can be particularly severe. Unless the AMA can change the FTC's mind, the Red Flag Rules will become effective on August 1 and those physicians who fit within the definition of "creditor" will be expected to comply.

The Red Flags Rule imposes obligations on "creditors" to detect, prevent and mitigate identity theft by developing a written identity theft prevention program. The term "creditor" is defined to include any

entity that regularly defers payments for goods or services or arranges for the extension of credit. According to the FTC a physician is a "creditor" if he or she agrees to bill the patient's health insurance first, but later bills the patient for amounts not covered by insurance including co-payments, coinsurance, deductibles and services not covered by insurance.

The Red Flags Rule requires the development and implementation of a written identity theft prevention program. The program must include reasonable policies and procedures to (i) identify the relevant red flags (a "red flag" is a pattern, practice or activity that indicates the possible existence of identity theft); (ii) explain the process for detecting red flags; (iii) describe how the practice will respond to any red flags that are detected; and (iv) describe how the program will be kept current.

The Rule's program requirements are risk-based, meaning that the steps entities must take to address potential identity theft should match the risks that they encounter. For example, the risk of identity theft may be low for a small medical practice in which the patients are familiar to the physician and staff. In that case, an appropriate program may consist of checking

identification and having procedures in place in case the office is notified that the patient's identity has been misused.

Note that although there are no criminal penalties for failing to comply with the Red Flags Rule, violators may be subject to financial penalties of up to \$2,500 per "knowing" violation.

Fortunately, there are several useful, easy-to-use sources available to help physicians develop an identity theft prevention program. The AMA has prepared a guidance document, along with sample policies, which can be

found under the heading "Red Flags Rule Resources" at [www.ama-assn.org/go/pmc](http://www.ama-assn.org/go/pmc). In addition, the FTC provides a template for organizations at low risk for identity theft – like many medical practices – to create their own identity theft prevention program under the heading "Create Your Program" at [www.ftc.gov/redflagsrule](http://www.ftc.gov/redflagsrule).

---

*Bruce E. Wood, Esq., is a shareholder of Wood & Smith, P.C. of Syracuse, New York, concentrating his practice on health law issues affecting physicians.*