



Understanding Red Flag Rules

Joseph Vance and Casey Moriarty

Health care providers are subject to a complex and multifaceted regulatory environment.

Laws such as the Health Insurance Portability and Accountability Act (HIPAA), Stark Law and the Anti-Kickback Statute, not to mention professional licensing requirements, provide a challenge to health care professionals who must scrutinize their business practices to ensure compliance. As of Nov. 1, providers are now subject to a new set of regulations known as the Red Flag Rules. (*editor note: Compliance deadline is now June 2010*)

The Red Flag Rules were designed by the Federal Trade Commission to combat the increasing risk of identity theft. According to the rules, all creditors with "covered accounts" must have policies to prevent and mitigate cases of identity theft involving their customers. The American Medical Association has argued that the rules should not apply to health care entities because they are not creditors in the traditional sense of the word. However, the FTC recently confirmed that any health care provider that bills an insurance company before billing a patient, or accepts payment after the day the patient receives services, must create an identity theft policy.

To comply with the rules, an identity theft policy must have procedures to identify possible indicators of identity theft, detect these red flags in the company's daily business and be able to respond to incidents. An entity must have this policy approved by its board of directors or the highest level of management and must ensure that it is periodically updated when new risks are discovered.

To ensure compliance with the Red Flag Rules, providers must review past experiences of identity theft and brainstorm about possible scenarios that might point to an identity thief at work. Examples include items in a medical record revealing treatment that is inconsistent with a patient's medical history, a patient's claim that he or she is a victim of identity theft, a patient who has an insurance number but cannot produce an insurance card or other identification and mail that is repeatedly returned even though transactions continue on the account associated with the address.

The policy also must include procedures for staff to detect red flags. Employees should be checking identification from all new patients, watching for inconsistent treatments described in medical records and monitoring accounts for which mail is repeatedly returned.

Finally, the policy must have procedures for responding to detected red flags. Proper responses include monitoring a suspect account, closing an account, or doing nothing if an investigation shows no presence of identity theft.

It is important to realize that the Red Flag Rules apply to all health care providers that extend credit to patients - even those who are already in compliance with the HIPAA Privacy and Security Rules. This is because HIPAA focuses primarily on the security and privacy of data, while the Red Flag Rules focus on discovering security breaches and mitigating the damage that breaches cause.

While providers may view the Red Flag Rules as another unwelcome regulatory headache, the FTC has attempted to ease the compliance burden. For example, smaller health practices with a low risk of identity theft need only fill out a six-page policy form available online at FTC.gov. But be warned: providers that fail to comply with the Red Flag Rules may be subject to fines up to \$2,500 and payments of \$1,000 to patients for each violation.

For providers that allow patients to defer payment for services, investing time today in preparing a thorough identity theft policy could be the key to saving money and headaches in the future.

Joseph Vance is a partner and litigation team chair for the Vancouver law office of Miller Nash LLP. He can be reached at 360-699-4771 or joe.vance@millernash.com

Casey Moriarty is an attorney and member of the healthcare practice team in the Seattle law office of Miller Nash LLP. He can be reached at 206-622-8484 or casey or moriarty@millernash.com