

**May, 2010**

## **The Red Flags Rule and Your Practice**

If it hasn't already, your practice should take steps to comply with the Red Flags Rule. The rule is a measure under federal regulations to curtail identity theft. In practical terms, your practice needs to develop and implement a written program that allows your staff to reasonably identify and respond to attempts to use stolen personal information.

### **Why Does the Rule Apply to Medical Practitioners?**

The Red Flags Rule generally applies to businesses that qualify as "creditors" in that they provide goods or services without requiring full payment up front. Since health-care providers typically bill patients and insurance companies after they have seen and treated their patients, they are required to comply with this new rule. Hospitals, nursing homes, and other medical institutions also must comply.

### **Compliance**

As a first step, your practice may decide to assign a team of employees to assess the areas of your operations that are vulnerable to identity theft. This assessment could involve reviewing your current procedures for handling the personal and financial data of patients and identifying weaknesses in your systems that could permit either the theft of patient identities or the use of stolen identities to obtain medical services. For example, the risk assessment could examine:

- How you verify the identity of an individual when he or she first becomes a patient
- What information you gather on that individual
- How you store that data after it has been collected
- The warning signs of possible identity theft (essentially, these red flags are patterns or activities that point to the existence of identity theft)
- The potential ways identity thieves could take advantage of your patients' relationships with your practice
- What steps could be taken to detect and prevent identity theft relating to existing accounts
- The likelihood, possibly ranked on a scale, of each specific risk occurring
- Whether existing controls, i.e., for HIPAA, can be incorporated in the compliance plan

## **Put the Plan in Writing**

Your risk assessment team should identify how someone might steal an identity in your particular situation. Also recognize that, over time, criminals will figure out other, more creative ways to steal a person's identity or to use a stolen identity for illegal purposes.

Once the risk assessment has been completed, your team should draft appropriate responses to each identified red flag. The risk assessment and the agreed-on responses to red flags should be discussed and documented thoroughly.

Next, your team should put your practice's identity theft program in writing. The regulations require that you be able to demonstrate reasonable policies and procedures to detect, prevent, and mitigate identity theft in connection with a covered account.

The written program must be submitted to an "administrator" (a board of directors, a designated committee of the board, or senior management) for review and approval. The person or persons with responsibility for overseeing the program should report to the administrator at least annually regarding compliance.

. . . demonstrate reasonable policies and procedures to detect, prevent, and mitigate identity theft . . . .