Health Information Compliance Alert

Identity Theft: Get the Right Facts in Your Red Flags Program -- And Be All Set for the May 1 Deadline

These sample items can help you shape your practice's policy.

You've got just two months to implement your red flags program, and help is on the way.

If you're just getting your feet wet in implementing an identity theft program to comply with the Red Flags Rule,we've got some tips that can make the process a little easier,courtesy of **Barbara Colburn,** director of operations for a medium-sized billing service in Wisconsin, and president of Total Health Care Solutions, a healthcare consulting firm.

1. Identify what the program is and who is affected. Your plan should outline why the practice members need to know about the rule and name all of the covered entities (offsite facilities, labs, clinics, etc.)

2. Identify 'red flags.'Make a list letting your staff know what they should be looking for regarding identity theft. For instance, they'll want to be on the lookout for potentially forged documents or an identification document with a photo, name, or age that doesn't appear to match the information on their insurance card.

In some cases, Colburn says, you may notice that several patients list the same phone number, address, or social security number. That's something you should investigate.Or the patient may refuse to fill out identifying information on his or her new patient registration form.

In other cases, the patient may give you his insurance information but is never able to produce the insurance card.

3. Keep billing in mind. Not all red flags will occur while the patient is present - some may crop up after the fact.

For example: You submit bills or other mail to a patient and you notice that the mail is repeatedly returned as undeliverable, although transactions continue to occur in connection with the patient's account.

4. Look for victims, too. In addition to watching out for perpetrators of identity theft, you should also be on the lookout for victims, Colburn advises.

For instance: Someone might complain about receiving a collection notice from your practice, even though she's never been there. Or she might find that she's reached her cap on her insurance benefits, even though she hasn't seen the doctor all year.

5. Take action. Your red flags program must list the steps that your employees should take if they detect a redflag event.

For instance, if your practice has a privacy officer on staff, you might have the staffers report the breach to that officer first. Or you might have them enter the information in the red flags database first - the important thing is that you establish a process so you can alert the board of directors of how you'll handle the breach.

In some cases, you might quickly contact the patient; in other instances, you may feel the need to notify law enforcement immediately - your red flags plan should cover all of the possible responses to a red flags breach.

6. Head off breaches. Your red flags plan should outline how you can prevent identity theft in your practice.

For instance, you might institute a policy of scanning a copy of the patient's photo identification on each visit,Colburn suggests.

Important: Don't refuse care or delay treatment for any reason for patients in emergency situations just because they've forgotten their photo ID or other identifying document.You are required to treat these patients under the EMTALA law.