The Red Flag Rules:
How does Dr. Leigh protect you from identity theft?

Background:
The Federal Trade Commission (FTC) has a rule, in place since 1/1/2008, requiring doctors, who they define as "financial institutions and creditors," to verify government-issued photo ID's, and possibly run credit checks, on all their patients. Why? To prevent "medical identity theft."

What is medical identity theft? From the New York Times (Walecia Konrad, 6/12/2009):

> *"Medical identity theft takes many guises... Someone can use stolen insurance information, like the basic member ID and group policy number found on insurance cards, to impersonate you - and receive everything from a routine physical to major surgery under your coverage... When people are not aware their medical identities have been stolen, insurance companies may simply continue to pay the fraudulent claims without the victim's knowledge. The person might learn of the fraud only when trying to make a legitimate claim, and the insurance company informs them they have reached their lifetime cap on benefits. Or victims may eventually discover erroneous information in their medical files during a doctor or hospital visit. And that may pose a bigger danger than the financial risks. The medical records may now contain vital information like blood type, allergies, prescription drug use or a history of disease that is just plain wrong. In an emergency, doctors could treat you based on this erroneous information.*
>
> *"And there are none of the consumer protections for medical identity theft victims that exist for traditional identity theft. Under the Fair Credit Reporting Act, you can get a free copy of your credit report each year, put a fraud alert on your account and get erroneous charges deleted from your record. If your credit card is stolen and the thief goes on a spending spree, you're not liable for more than $50 worth of the charges. With medical identity theft, though, the fraudulent charges can remain unpaid and unresolved for years, permanently damaging your credit rating. Under the federal law known as HIPAA - the Health Insurance Portability and Accountability Act - you are entitled to a copy of your medical records... [but] HIPAA privacy rules can actually work against you. Once your medical information is intermingled with someone else's, you may have trouble accessing your files. Privacy laws dictate that the thief's medical information now contained in your records must be kept confidential, too. Even when you are able to correct a record, say in your doctor's office, the erroneous information may have been passed on to dozens of other health care providers and insurers. Victims must track down and resolve these errors."*

According to the FTC website, all physicians must establish a formal identity-theft "red-flag" identification program. The FTC suggests checking a photo ID for each "encounter," and also suggest that physicians run a credit check on each patient, too.

If a doctor is found to be "noncompliant" with these directives (in other words, if they don't have a written "red flag" plan, implemented and regularly updated "to respond to emerging threats"), they can be fined $2,500 for each time they "extended credit" (sent a bill or collected a copay). If they already received a warning and are still noncompliant, the fine is $11,000 "per incident." States can add on their own additional penalties.

Identity theft is very bad; everyone is against identity theft! However, I doubt patients will appreciate being obliged to show a photo ID, with a correct current address and a photo matching their current appearance, every time they go to the doctor. I intend, as your personal physician, to get to know you and your family well, so that I would notice immediately if someone else pretended to be you for the purposes of medical care. This should make it unnecessary to check a photo ID other than when we first meet. I do not intend to routinely, if ever, "run a credit check" (I don't even know how to do it).

Here are Dr. Leigh's Red Flag Rules:

What's a red flag?

These shall be considered as red-flag events and possible indications of medical identity theft:

1. Alerts, notifications and warnings from credit reporting agencies or service providers (for example, insurance companies), such as report of fraud, of a credit "security freeze", or of a very unusual pattern of activity of a patient account (for example, sudden multiple trips to different emergency rooms).

2. Questionable documents, such as an ID that appears to be forged, an insurance number but no insurance card or documentation, or a signature that appears forged.

3. Questionable identity information, such as inconsistent names or birth dates, an invalid phone number or fake billing address, the same name and birthdate used by more than one patient, or refusal to give any identifying information.

4. Questionable billing-account or medical-record activity. For example, payments stop on an account that is usually up to date, mail sent to the patient is repeatedly returned as undeliverable, a breach in Dr Leigh's computer system security, or medical records showing treatments that don't match a physical exam (such as mismatches in age, race, blood type, etc).

5. Alerts from patients: patients who get a bill for somebody else's medical care, a bill or insurance notification for care they didn't get, a bill from a doctor they've never seen, a warning from a collection agency that the patient thinks is a mistake, a problem on their credit report that they think is a mistake, a problem with insurance (example, benefits have been all used up) that they think is a mistake.

6. Alerts from others: including police investigating a case of identity theft in which the patient is involved somehow.

Where might we see a red flag?

1. New Accounts.

When I see you as a new patient, unless you're paying the full doctor fee in cash at the time of service, I will verify and enter into your medical record:

- Your name (Please bring a current ID, driver's license, or passport to your first visit)
- Your date of birth (Please bring a current ID, driver's license, or passport to your first visit)
- Your current address (Please bring a recent piece of mail with your address on it)
- Your insurance information (Please bring your insurance card or policy)
- Your insurance coverage (I might need to call your insurance company to find out information like deductibles and copays, if you don't know them)
- Your job address, if your insurance is through your job
- Your photo (Your medical record can store your photo, so that nobody can pretend to be you)

Please bring these documents even if you are not the patient, but you are responsible for the doctor bills.

2. Established accounts.

I will always verify the identity of any patient asking for information or records, whether in person, by phone, by fax or by email. I will also verify identity before honoring any request to change a billing address, to change credit card information, or to change other billing information.

What can we do?

If red flags were to appear, Dr Leigh would do one or more of the following, depending on the kind of red flag and the risk it represents:

1. Prevent/ respond

Notify patients immediately if there is a breach of computer security
Change any passwords that permit access to an account
Notify local or national law enforcement if necessary
Notify the Postal Service Inspection Service if necessary
Continue to monitor the account in question, for red flags
Refuse to open a new account, and/or hold further transactions until red flags are resolved
Not attempt to collect on an account that has red flags
In some circumstances, no action may be needed

2. Protect identity information

Dr. Leigh's HIPAA Privacy Rules will be followed, and will be updated along with these Red Flag Rules, as needed, to improve protection.

3. Protect medical information

If medical identity theft occurs, there may be errors in the patient's chart as a result. Bad information may have been added to an existing chart, or the contents of an entire chart may refer only to the health condition of the identity thief (under the victim's name and other identifying information). In such cases, Dr. Leigh will take appropriate steps to avoid medical mismanagement due to bad information, such as file extraction, correction, cross-referencing charts, etc.

4. Red flag rule updates

Dr. Leigh will periodically and/or yearly review and update these rules to reflect any new risks for identity theft, considering previous experience with identity theft, changes in methods of identity thieves, changes in methods of detecting, preventing, and mitigating identity theft, changes in types of patient accounts, and changes in business relationships with other agencies.

Resources:

- Oregon's Information Security Resource Center: http://www.oregon.gov/DAS/EISPD/ISRC/index.shtml
- Oregon's site on Identity Theft: http://www.oregon.gov/DAS/EISPD/ISRC/topics_idtheft.shtml#OCITPA___The_Oregon_Consumer_Identity_Theft_Protection_Act
- About the Oregon Identity Theft Prevention Act: http://www.cbs.state.or.us/dfcs/id_theft.html
- Paypal's Identity Theft Prevention site: https://www.paypal.com/cgi-bin/webscr?cmd=_security-center-outside
- The Federal Trade Commission's site on Identity Theft Prevention: http://www.ftc.gov/bcp/edu/microsites/idtheft/

Updated July 2009
Leigh Saint-Louis, MD, LLC