Medical Identity Theft and the Red Flags Rule

Save to myBoK

by Chris Apgar

Continuing our Health Information Privacy and Security Week series, today Chris Apgar, CISSP, president of Apgar & Associates LLC, takes a look at medical identity theft within the context of the Red Flags Rule.

Much is reported in the news about identity theft including new catchy commercials that are intended to prompt consumers to pay attention to their credit record. What isn't mentioned is the threat of medical identity theft. Identity theft is primarily a financial crime while medical identity theft can directly impact an individual's ability to seek healthcare and health insurance coverage.

Medical identity theft can result in the thief obtaining expensive health services under someone else's name or purchasing insurance coverage based on someone else's clean bill of health. When the bills come due, the provider will look for payment from the individual who was the victim of medical identity theft.

When attempting to purchase insurance, the individual with the clean bill of health may find charges for, say, chronic conditions of the thief, which results in the individual finding insurance coverage is no longer available or is very expensive.

New regulations will soon be in force that will require certain organizations implement programs to prevent identity theft and medical identity theft. The new regulations, the Red Flags Rule, are a result of the Fair and Accurate Credit Transaction Act of 2003. The new regulations are effective May 1, 2009.

The regulations, published and to be enforced by the Federal Trade Commission, affect organizations classified as "creditors." Creditors are organizations that maintain consumer accounts that are classified under the rule as "covered accounts."

An account is a covered account if partial payment is made with an additional payment made later or when multiple payments for a given service or product occurs. This does not include credit card companies.

In the medical world, most providers are considered creditors because they maintain patient accounts where multiple payments are made. As an example, a patient receives medical services, the provider bills the insurance company and later bills the patient for the balance.

The rule doesn't just cover what are classified as covered accounts. If a provider even has one covered account, the provider is required to implement an identity theft protection program that includes all patient accounts.

The purpose of an identity or medical identity theft protection plan is to identify flags or triggers that would indicate identity theft may be occurring. As an example, if a patient presents what appears to be altered or forged identification, that would be a flag. If a new patient provides the same billing address as an existing patient (and is not family), that is another flag. The purpose is to take steps to prevent identity and medical identity theft from occurring rather than finding out after the fact.

This directly ties with existing breach notification laws and the HIPAA security rule requirement to form a security incident response team. The team would likely be responsible for following up on reported flags. The breach notification laws are the other side of a protection program. The Red Flags Rule is intended to be preventive while breach notification requirements are reactive.

Most provider and some health plans are required to comply with the Red Flags Rule effective May 1 this year. If the Red Flag class of "creditors" has not started preparation to comply, time is quickly running out.

Original source:
Apgar, Chris. "Medical Identity Theft and the Red Flags Rule" (Journal of AHIMA website), April 2009.