Red Flags Rule: Protecting Providers and Patients from Medical Identity Theft

Steven Toporoff offers tips on complying with the Red Flags Rule, which goes into effect May 1. Toporoff works in the FTC's Division of Privacy and Identity Protection, Bureau of Consumer Protection.

Millions of Americans each year fall victim to identity theft. When identity theft involves healthcare, the consequences can be severe. It can result in losses to the healthcare provider from unpaid bills, the exhaustion of the victim's benefits, or even potentially life-threatening corruption of a patient's medical records.

The crime also can play havoc with an innocent consumer's credit rating. Medical identity theft may arise when a person seeks healthcare services or prescription pharmaceuticals using someone else's name or insurance information. A recent nationwide survey conducted for the FTC found that 4.5 percent of the 8.3 million identity theft victims have experienced some form of medical identity theft.

The Red Flags Rule is designed to help protect patients and providers from suffering the consequences of medical identity theft. Briefly put, this new law requires "creditors" and "financial institutions" to determine if they have either consumer accounts that permit multiple payments or other accounts for which there is a reasonable risk of identity theft. If they do, these covered entities must develop and implement a written identity theft prevention program. Each provider has the flexibility to implement a program that best suits its size, complexity, and actual risk of identity theft.

Although enforcement has been deferred until May 1, 2009, many providers are already putting their programs together. Some, however, question the applicability of the rule to physicians and other providers, because they do not view them as "creditors." For purposes of the Red Flags Rule, the definition of "creditor" is very broad, and includes an arrangement for the deferral of payment of debts or payment for the purchase of goods or services. Healthcare providers are creditors if they regularly collect payment after services are rendered. Simply accepting credit cards as a form of payment, however, does not make a provider a creditor under the rule.

The first step in implementing a program is to identity the warning signs—or "red flags"—of identity theft. These may include identification, medical history, or information that does not seem to match the patient, or notice from consumers that they are victims of identity theft. Second, the program must include policies and procedures to detect these "red flags." For example, many providers already check a photo ID or insurance information for new or returning patients.

Third, the program must include appropriate responses to prevent and mitigate identity theft. These could include not collecting on a debt against the innocent consumer or ensuring that medical records are not corrupted with errors resulting from the identity theft. Finally, providers must update their programs periodically if new risks and trends arise. To ensure that these steps become routine, the rule requires that the Red Flags Program be in writing.

Using this common-sense approach to developing a program can help reduce the incidence of medical identity theft without overburdening health care providers. And because the rule is risk-based, a simple plan should be sufficient for providers that have a low risk of identity theft in their practices. Still have questions? Send a message to redflags@ftc.gov or check www.ftc.gov for more information.

Original source:
Toporoff, Steven. "Red Flags Rule: Protecting Providers and Patients from Medical Identity Theft" (Journal of AHIMA website), April 17, 2009.
