

GOVERNMENT & MEDICINE

Caught unaware, doctors get delay in FTC enforcement of ID theft rules

The AMA and other groups won a six-month reprieve for doctors to implement a prevention program originally mandated for Nov. 1.

By [Amy Lynn Sorrel](#), *AMNews* staff. Nov. 3, 2008.

New Federal Trade Commission regulations to combat identity theft have taken physicians and the health care industry by surprise and prompted the agency to delay enforcement from Nov. 1 to May 1, 2009.

The so-called "red flag" rules require entities that regularly extend credit, or defer payment for services, to establish a written program for preventing identity theft as well as detecting and responding to warning signs of such thefts. The commission first released the rules last November as directed by the Fair and Accurate Credit Transactions Act of 2003.

Until recently, physicians and health care facilities were largely unaware of the regulations, which were thought to pertain mainly to banks and other financial institutions that offer credit in the traditional sense. But in recent weeks, the FTC signaled that the rule was intended to apply more broadly, including to the health care arena.

"In the context of health care, medical identity theft is not just a financial matter. It can have real consequences for physical harm to patients," said Naomi Lefkovitz, an attorney with the FTC's Division of Privacy and Identity Protection. "For doctors, [a prevention program] can be especially important, because they might not realize or figure out who is an identity thief until after they provide services."

The rules -- released in conjunction with the U.S. Dept. of Treasury, the Federal Deposit Insurance Corp. and other federal financial oversight agencies -- largely discuss banks, mortgage brokers, auto dealers and other lenders with only a single mention of medical identity theft.

"The vast majority of health care providers did not see this on the radar," said Gerald E. DeLoss, vice chair of the American Health Lawyers Assn.'s Health Information & Technology Practice Group. The trade organization held a conference Oct. 1 to discuss the regulation.

Most physicians and group practices likely will fall under the FTC's definition of a creditor because they generally do not collect payment at the time a service is rendered and often hold off billing patients in full, according to legal experts. While accepting credit card payments does not apply in this case, such routine practices as setting up a payment plan or billing an insurance company before charging the patient likely do.

"If, on a regular basis, a physician allowed a patient to leave knowing they were not going to be paying immediately, even for a co-payment or deductible, the provider would be considered a creditor," DeLoss said.

The rules apply to creditors who maintain so-called covered accounts, designed to handle multiple transactions as part of an ongoing relationship. The FTC also defines a covered account as one involving a "foreseeable" risk of

identity theft. For physicians, that means most billing accounts, DeLoss said. While medical records generally do not qualify, they could be included if they are commingled with financial accounts.

A new deadline for physicians

The American Medical Association and more than two dozen national and specialty medical associations are challenging what physicians consider the FTC's overly broad interpretation of the 2003 statute. In a Sept. 30 letter, the groups asked the agency to clarify its position and delay enforcement of the rules until it does.

Physicians should not be considered creditors "simply because [they agree], after the fact, to let the patient pay in installments as opposed to turning the matter over to a collection agency or suing the patient," the letter states. In addition, billing an insurer first does not necessarily mean a patient is in debt for the remainder while the claim is processed, it states. The AMA and the other organizations pointed to appeals court decisions to suggest that the commission's interpretation should not include physicians as creditors.

On Oct. 22, the FTC relented and announced that it would not enforce the rule for six months because it learned that certain entities were not aware that they would be subject to the regulations.

"The commission's delay of enforcement will [give] these entities sufficient time to establish and implement appropriate identity theft prevention programs," the agency said in a statement.

When the FTC begins enforcing the rules, failure to comply could mean administrative penalties or up to \$2,500 in fines per violation.

Questions persist as to whether the red flag rules overlap with the Health Insurance Portability and Accountability Act. The AMA letter to the FTC suggested that the agency failed to consider the additional legal and administrative burdens the new rules impose when HIPAA already requires them to keep patient information private and secure.

Some legal experts said the red flag rules go even further than HIPAA.

"HIPAA covers how an entity uses and discloses protected health information" to avoid unauthorized breaches, said Heidi Y. Echols, a partner at the law firm McDermott Will & Emery in Chicago. But the red flag rules add another layer of protection by requiring doctors to respond to evidence of medical identity theft even when it is presented to a physician's office after a patient's information has been stolen from elsewhere.

The red flag rules also focus on financial matters, whereas HIPAA primarily addresses medical records, noted Pam Dixon, executive director of the World Privacy Forum, a public interest group.

Federal officials have not yet said whether a red flag rules violation also could amount to a HIPAA violation. The Dept. of Health & Human Services Office for Civil Rights, which enforces HIPAA, said it is still analyzing the issues raised by the new requirements.

Keys to prevention

In the meantime, experts recommend that physicians seek legal counsel regarding compliance. Making the required changes might not be difficult.

While a compliance program likely will involve some time and expense, doctors may be able to build off HIPAA procedures already in place, Echols said. "This may be another thing added to the to-do list for doctors ... but it is something designed to protect patients."

The rules mandate implementation of a formal program with "reasonable" policies and procedures for recognizing and mitigating patterns, practices or activities that could signal identity theft. The plan, which requires senior

management approval, adequate staff training and periodic review, can be tailored to each physician's practice, Lefkovitz said.

Dixon also recommended that physicians revisit internal security policies that could open the door inadvertently to medical identity theft. For example, many practices are reluctant to give patients a copy of their medical records even though that could create an opportunity to identify discrepancies and errors.
