ID Theft Prevention Programs Are New Necessity

BY MARY ELLEN SCHNEIDER

Physicians and health care organizations must now implement a formal identity theft prevention program to protect their patients under a little-known set of regulations called the "Identity Theft Red Flags Rule."

The rule, which was issued by the Federal Trade Commission (FTC) in 2007 but will be enforced starting this month, is aimed primarily at creditors and financial institutions. However, after publication of the rule, the FTC informed physician groups that it was interpreting the term creditor broadly to include health care professionals who regularly allow consumers to defer payment for services. Therefore, any medical practices that allow patients to defer payment while they bill insurance would be covered under the rule.

Physicians and other health care professionals are required to come into compliance with the rule as of May 1, 2009.

The rule requires health care professionals to develop and implement a written identity-theft prevention and detection program to protect consumers. Specifically, the rule calls for organizations to conduct a risk assessment to determine their vulnerability to identity theft. Next, they must develop and implement a written identity-theft program to identify, detect, and respond to those risks.

As part of the plan, organizations must specify how they will detect the "red flags" alerting them to potential identity theft. The program also must include how the organization will respond once a red flag is detected.

While identify theft is most commonly associated with financial transactions, there is increasing concern about identity theft in the health care sector, according to the FTC. For example, medical identity theft can occur when a patient seeks care using the name or insurance information of another person.

For most physicians working in settings with a low risk for fraud, an identity-theft program could be simple, according to the FTC. For example, staff at the practice could check a photo identification at the time services are sought. Another part of a basic program would be to develop steps to take in the event that someone's identity has been misused. That might include not collecting debt from the "true consumer" and not reporting the debt on the consumer's credit report. Also, practices should ensure that the correct medical information is in the patient's chart, according to the FTC.

But the interpretation of physicians as creditors has raised the hackles of the American Medical Association, the American College of Physicians, the American College of Emergency Physicians, the American College of Surgeons, the American Academy of Pediatrics, and several other physician organizations. Those groups contend that physicians are being inappropriately labeled as creditors, and that the requirements place an undue burden on physicians that could adversely affect patients' access to services.

Another objection that many physician groups have to the Red Flags Rule is that they didn't have an opportunity to comment on its impact before it was issued. Since the 2007 rule didn't explicitly mention physicians, the AMA and others contend that the FTC must publish a new rule and put that new rule out for public comment.

"The FTC did not give physicians an appropriate opportunity for notice and comment on the ruling that the Red Flags would be applied to them," Dr. Ardis D. Hoven, an AMA board member, said in a statement. "The AMA is calling on FTC to republish its rule so that we can make the case that physicians should be excluded from the Red Flags Rule." ■

A Federal Trade Commission guide explains how to comply with the red flags rule (www.ftc.gov/bcp/edu/pubs/articles/art11.shtm). The American Medical Association offers guidance at www.ama-assn.org/ama/no-index/physician-resources/red-flags-rule.shtml. A 30-page report from the World Privacy Forum explains the rule and offers suggestions for providers (www.worldprivacyforum.org/pdf/WPF_RedFlagReport_09242008fs.pdf). The Federal Register notice is at http://edocket.access.gpo.gov/2007/pdf/07-5453.pdf.