

# Plan Generating Criticism

Certification from page 1

Board of Medical Specialties (ABMS) to create certification for the subspecialty of procedural dermatology. The American Society for Mohs Surgery took an early stand against the proposal and others followed.

Last month, the ABD was scheduled to submit a revised application to the ABMS Committee on Certification and Recertification but postponed on the advice of ABMS officials. In the meantime, the ABD has formed its own task force to review areas of concern raised by critics and to report back to the group's

board of directors in December with specific recommendations.

Around the time that the ABD announced it was postponing its application, the American Academy of Dermatology also came out against the proposal. During an Aug. 1 meeting, the AAD board of directors approved a resolution opposing the ABD's proposal.

The American Society for Mohs Surgery, which has been critical of the move toward certification, is taking a wait-and-see attitude. Dr. Stephen Spencer, president of the society,

said it will monitor the situation and evaluate a new proposal if and when it comes forward.

Despite the criticism, the ABD continues to argue that subspecialty certification in procedural dermatology is important both for patient care and for the specialty of dermatology.

There is a body of knowledge related to surgical and procedural dermatology that is not taught in dermatology residency programs and subspecialty certification would offer assurance to patients that the physician is qualified and possesses the necessary knowledge, experience, and skills. The specialty would also gain under the proposal because certification would estab-

lish surgery as an integral part of dermatology, according to ABD.

The ABD's board rebuts charges that subspecialty certification will lead to economic credentialing. Since certification would be voluntary, the lack of a subspecialty certificate would not indicate that a physician is unqualified to practice in the specialty, the ABD said.

Some critics, however, aren't satisfied with the ABD's assurances. Dr. Daniel E. Gormley, a dermatologist in Glendora, Calif., said that, as currently written, the ABD's proposal would only grant certification to dermatologists who have completed fellowship training in procedural dermatology, out-

side of those who would be grandfathered in. Eventually, only a small group of dermatologists would be certified to perform a wide range of procedures, he said.

Dr. Gormley said the main issue with the ABD proposal is that it will restrict the number of dermatologists who can perform Mohs surgery and related procedures. Instead of creating a small cadre of specially trained dermatologists, he said that all dermatology trainees should have the opportunity to learn these procedures during their residency.

"We want to share this knowledge and spread it around," Dr. Gormley said. ■

# Experts Offer Advice on Complying With the Red Flags Rule

BY JOYCE FRIEDEN

WASHINGTON — The federal Red Flags Rule that requires creditors to check for identity theft may mean a few new procedures for office-based physicians, Patricia King said at the American Health Lawyers Association's annual meeting.

"Do health care providers have to comply with the Red Flags Rule? Yes, if they're [considered] creditors," said Ms. King, assistant general counsel at Swedish Covenant Hospital in Chicago.

The rule requires creditors to establish formal identity theft prevention programs to protect consumers. Aimed primarily at the financial industry, the regulation was originally scheduled to go into effect on Nov. 1, 2008. However,



to give small businesses more time to prepare for compliance, the Federal Trade Commission (FTC) delayed enforcement until May 1, and then until Aug. 1, and most recently until Nov. 1.

Earlier this year, the AMA and physician specialty societies argued that physicians are not creditors because they bill insurance companies, not individual consumers, Ms. King said. "But the patient does get billed for copays, deductibles, and excluded services, so unless all those charges are collected up front, the health care provider is billing and possibly deferring payment for the cost of services."

To address providers' concerns, the FTC has published guidance and developed a template for identity theft prevention program for low-risk creditors. (Information available at [www.ftc.gov/bcp/edu/pubs/articles/art11.shtm](http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm).)

Low-risk providers who see the same patients regularly can adopt a simple identity theft program, she said, adding that personnel involved with front desk, medical records, and patient account functions should be involved in the program.

Physicians need to identify which patient accounts will be covered by the

rule—such as those patients who need to make repeat payments—and develop appropriate policies and procedures, Ms. King said. "The final [Red Flags] rule had 26 examples of identity theft. Look through them and see which ones are most applicable to you."

Providers also need to look at what information they collect when patients register. "Many of us need to re-think our standard registration procedures and beef them up," said Ms. King. One example might be to ask for a photo ID.

Procedures to fight identity theft need to be approved by the organization's board of directors and overseen by senior management, according to the rule, "because this is intended to be a high-priority program, not something that's delegated to a lower-level manager," she said.

Typical "red flags" include:

- ▶ Insurance information that cannot be verified.
- ▶ No identification.
- ▶ A photo ID that doesn't match the patient.
- ▶ Documents that appear to be altered or forged.
- ▶ Information given that is different from information already on file.
- ▶ An invalid Social Security number.
- ▶ A patient who receives a bill or an explanation of benefits for services he or she didn't receive.
- ▶ A patient who finds inaccurate information on their credit report or on a medical record.
- ▶ A payer that says its patient information does not match that supplied by the provider.

When a patient raises one or more red flags, the practice has two options. It could refuse to provide service, although this might raise a problem under the Emergency Medical Treatment and Labor Act, which prohibits providers from not treating persons with questionable identification who require emergency care.

Or the practice could provide the service, but ask the patient to bring in the correct information to his or her next visit. Ms. King cautioned providers about freely providing medical records to a patient suspected of identity theft, because it could lead to more identity theft.

Patients will have to be educated about the new rule, Ms. King said. "Providers are going to run into problems with patient expectations. Patients have gotten used to coming to their doctor ... with either no identifying documents or only their insurance card. They will need some education in advance."

She encountered a case of identity theft at her own hospital involving two elderly women, one of whom had a public assistance card, while the other one didn't. They thought it would be okay if the woman without the card used her friend's card. The identity theft was discovered by a hospital radiologist who noticed that the women's scans were different.

Providers also should note that com-

pliance with the Health Insurance Portability and Accountability Act (HIPAA) does not shield them from complying with the Red Flags Rule.

"One of the questions we get is, 'I already comply with HIPAA; aren't I done?'"

The answer is, 'Probably not,' said Naomi Lefkowitz of the Federal Trade Commission's division of privacy and identity protection. "The Red Flags Rule is really about fraud protection, and HIPAA is more about data security. There is certainly some overlap, and to the extent that, for example, someone is checking photo IDs ... to make sure that the person only has access to their [own] medical record, that's a policy that might do double duty under the client's identity theft program as far as verifying ID ... Having the HIPAA program is probably not going to make [providers] compliant."

MS. LEFKOWITZ

MS. LEFKOWITZ

Mary Ellen Schneider contributed to this article.

