



PROFESSIONAL ISSUES

Medical identity theft is often an "inside job"

Asking patients for photo IDs is one safeguard, but many thefts are also committed by health care employees.

By [Beth Wilson](#), *AMNews* correspondent. March 3, 2008.

When physicians look to protect their patients from medical identity theft, they may want to start by examining their office staff.

That's because, while patients may try to use another person's identity fraudulently to receive medical care, many thefts happen when a hospital, clinic or practice employee sells patient information to organized crime or gang leaders, experts said. Then the information is used to conduct fake billing or obtain goods such as wheelchairs and prescription drugs to sell on the black market, said Pam Dixon, executive director of the World Privacy Forum, a nonprofit research and consumer education organization.

- See [related content](#)
- [E-mail](#) - [Print](#)

The forum is conducting its second study of medical identity theft, and the findings will be released later this year. In its first study, issued in 2006, the organization reported that 250,000 to 500,000 people had experienced this form of identity theft.

A 2007 study by the Federal Trade Commission estimated that medical identity theft affected about 250,000 people in 2005.

"We have the anecdotal information that it is increasing," Dixon said, noting that cases involving individuals committing the crime alone are rare. "We do see some of that where someone steals a wallet or they steal someone's name. That does happen. But the preponderance of cases are happening from insider jobs."

Dixon points to a case at the Cleveland Clinic in Weston, Fla., where Isis Machado, a front-desk office coordinator, pled guilty to selling information involving more than 1,000 patients. Although the hospital had browser controls to limit the number of records that employees could view, no one noticed Machado was exceeding that limit regularly, Dixon said. Machado's case resulted in \$7 million in Medicare fraud.

"It's a very profitable crime," Dixon said, adding that thefts happen most often in large institutions or at clinics. "We're looking at this as more of an insider threat."

Keeping information safe

Physician offices can help prevent medical identity theft by asking patients to provide photo IDs.

Gynecology & Laparoscopic Surgeons in Raleigh, N.C., began checking each patient's driver's license at registration after receiving warnings of identity theft from hospitals and calls from insurance companies asking for patient verification.

Lisa Roberts, MD, a gynecologist at the practice, has only encountered one case of identity theft, as a medical student, when an uninsured patient tried to use someone else's ID. "To my knowledge we haven't had a problem like that," she said, noting that the office policy of

checking driver's licenses may deter such acts.

Kimberly Melton, the practice's manager, said, "Word does get out that you're checking IDs."

At first, patients resisted, asking why the office needed to see a driver's license. But once office staff explained the move was designed to prevent identity theft, "it's become common, and patients are more willing," Melton said. But she said it's difficult to reduce the number of health care staff with access to patient Social Security numbers since that is how a patient who needs surgery or lab work is identified.

At Raleigh, N.C.-based WakeMed Health and Hospitals, employees at registration desks ask patients to provide a photo ID such as a driver's license or passport.

"Certainly there are times when they don't have those, and we register them anyway," said Heidi McAfee, WakeMed's director of patient access.

If patients don't provide Social Security numbers, the hospital asks for a phone number, address and date of birth, then sends an electronic query to a company to confirm the information. To reduce the chances of someone overhearing patient information, the hospitals added white noise above some registration booths and enclosed or partially enclosed some with walls and plastic glass.

The hospital group also is looking to change computer displays for its billing employees so they see only the last four digits of Social Security numbers, McAfee said.

Glenn Martin, MD, director of medical informatics for Queens Health Network in Queens, N.Y., said his network adapted a smart card system in August 2003 to prevent patient confusion and misidentification, given that more than 100 languages are spoken within a 10-mile radius of Queens Hospital.

Although the cards, which contain photos, lab results and other information, were not designed with medical identity theft in mind, they may add another layer of protection, Dr. Martin said.

[Back to top.](#)

Copyright 2008 American Medical Association. All rights reserved.

RELATED CONTENT *You may also be interested in:*

[Prying eyes: Protecting patient records](#) Oct. 1, 2007

[Fax sent by United subsidiary causes security concerns](#) May 14, 2007

[Safeguarding identity: Tips to stave off a growing problem](#) June 26, 2006

[Physicians being targeted in identity theft scheme](#) Jan. 31, 2005