

healthcare registration

ASPEN PUBLISHERS

June 2008 • VOLUME 17, NO. 9
EDITOR: LAURA J. MERISALO

Medical Identity Theft

Patient access first in line to manage the nation's fastest growing crime

Medical identity theft is a dangerous and fast-growing crime. Current estimates are that up to 250,000 patients have been victims of medical identity theft, and some estimate that the number of victims may be even higher, affecting as many as 500,000 patients.

Most simply, medical identity theft is when a person uses another individual's name, Social Security number, driver's license, insurance information, or other personal identification, without the individual's knowledge or consent, to obtain medical services, prescriptions, or other medical goods. It is a crime that may be perpetrated by an individual acting alone, or it may be perpetrated by sophisticated criminals. In instances when medical identity theft is perpetrated by sophisticated criminals, medical identity theft is the first step in a larger scheme to commit health care fraud for financial gain. Perpetrators steal patient identities to buy, sell, or use the identities to submit false claims to receive payment for medical services for conditions the victims never had and for services that were never provided.

Patients at Risk

The financial consequences and physical jeopardy caused by medical identity theft can be extreme. Victims of identity theft receive medical bills for hundreds if not thousands of dollars for care they never received. For instance, a Colorado man whose Social Security number, name, and address were stolen learned he was a medical identity theft victim when he received a bill for \$44,000 for a

surgery he never received.¹ In Pennsylvania, a medical identity theft victim learned an imposter had used his identity at five different hospitals, creating medical histories in the victim's name at each facility, and receiving more than \$100,000 in medical treatments.²

Horror stories that come to light in the aftermath of medical identity theft abound. One such horror story is the case of a young mother of four who was contacted by a hospital to report that her newborn tested positive for illegal drugs. The woman had not given birth in years. Rather, another woman used the victim's driver's license during admission to a hospital to deliver her baby.

The identity thief disappeared but the results of the thief's crime wreaked havoc in the victim's life. She found law enforcement officers at her door, alleging she was an unfit mother because she gave birth to a drug-addicted newborn and threatened to take her four children from her. She also received a \$10,000 bill for the labor and delivery hospital services provided to the thief. Today, she worries that her now-compromised medical records are forever tainted and that, one day, she may face a medical emergency and clinicians will rely on false medical information entered into her record by the medical identity thief.

One industry expert put the patient risks in medical identity theft in context with the hypothetical case of a victim who arrives in an emergency department with an acute case of appendicitis. The patient arrives with all the signs and symptoms of someone suffering appendicitis, but the medical record falsely shows the patient's appendix had been removed—from the medical identity thief! Thus, the patient is at risk while emergency personnel attempt to identify the cause for the patient's agony, and rely on an

inaccurate medical record to incorrectly rule out the possibility of appendicitis.

As the World Privacy Forum notes, medical identity theft is a crime that can kill. It is a crime that often goes undetected for months or even years, while victims' medical records are altered to reflect inaccurate medical conditions, blood types, drug allergies, and other health information relied upon to administer medical care. For the health care industry, medical theft poses significant financial jeopardy, as the resulting fraudulent claims can bilk public and private insurers of millions of dollars in losses each year.

Medical Identity Theft in Context

Medical identity theft is flourishing at a time when patient safety and patient privacy also are hot-button health care issues. Further, it is a crime that exacerbates both patient safety and patient privacy.

Patient safety gained the spotlight in 2000, with the publication of the Institute of Medicine's report, *To Err Is Human: Building a Safer Health System*, in which experts estimated that as many as 98,000 people die each year due to preventable medical errors.³ As the number of medical identity theft victims continues to escalate, the issue of patient safety takes on a new twist, as inaccuracies are introduced into patients' medical records due to medical identity theft, laying the foundation for potential medical errors that could prove tragic. The false information may belong to a medical identity thief who used the victim's identity to obtain medical services, or it may be false information fabricated by the thief who used the victim's identity to generate false claims for services, as part of a scheme to commit health care fraud and receive payments for services never provided. Because medical identity theft can remain hidden for months or even years, the end result is that this crime places patient safety at risk.

Patient privacy concerns led to the implementation of the privacy and security rules as part of the Health Insurance Portability and Accountability Act (HIPAA) of 1996.⁴ As it turns out, HIPAA is not a panacea to ensure patients' private and personal health care information is protected, particularly as the health care industry increasingly relies upon electronic health records for clinical and administrative functions. Indeed, it is difficult, if not impossible, to guarantee that access to and the fraudulent use of privileged, personal health care information is not violated.

Front-End Response

Although medical identity theft can be difficult to detect and thwart, particularly when perpetrated

by sophisticated criminals, there are steps health care provider organizations can and are taking to verify patient identities—for patient safety and to avert health care fraud. The onus is on providers to protect the people they serve, particularly as that is what health care consumers expect, as patients hold health care providers in positions of trust. Patients enter a health care system with a sense of security, believing that their personal medical issues and information are and will remain private, and that their medical records have been and will remain secure and reliable to ensure quality health care is delivered to treat their current illnesses or injuries.

As medical identity theft runs rampant, health care provider organizations, beginning at patient access, must take steps to improve and ensure the accuracy of patient identification. Indeed, accurate patient identification now tops the list of 2008 national patient safety goals issued by the Joint Commission. With the top 2008 patient safety goal being “to improve the accuracy of patient identification,”⁵ The Joint Commission offers the following suggestions to improve accurate patient identification:

- Emphasize with employees that the primary responsibility of health care workers is to check and verify the identity of patients;
- Use at least two identifiers to verify a patient's identity upon admission or transfer to a facility;
- Standardize the approaches to patient identification among different facilities within a health care system;
- Incorporate employee training on procedures for checking/verifying a patient's identity into the orientation and continuing professional development for health care employees; and
- Educate patients on the importance and relevance of correct patient identification in a positive fashion that also respects concerns for privacy.

Photo IDs Are a Critical Registration Data Element

Due to the threat of medical identity theft, many health care provider organizations require that patients provide photo identification at the time of registration or admission. Although a photo ID alone is no guarantee that patients are who they say they are (false driver's licenses to accompany a stolen medical identity are handily secured by sophisticated fraud perpetrators), it is an important step in the right direction.

At a Georgia medical facility, patient photo identification is required at registration and a patient's photo ID is then scanned into the system. If a patient presents for care without a photo ID and/or without a photo ID already scanned into the system, front-end employees take a picture of all patients—over the age of 18 or emancipated—to enter the photo ID into the record to help verify patient identity, to help ensure patient safety, and to help improve accurate patient account identification.

If patients do not have a photo ID on file and object to patient access employees creating a photo ID for the patient record, patient access employees are trained on how to respond to such patient protests. Most importantly, patient access employees are trained to inform patients that the photo ID is a patient benefit, to ensure that the right patient is receiving the right care and to ensure the correct patient account identification. If the patient still objects to having his or her photo taken and placed in the medical record, and if the patient is not in for emergency care services, front-end employees, in consultation with a supervisor, are trained to request that the patient reschedule the appointment at a time when the patient can present with a photo ID, as photo identification is required to process the registration.

Accurate ID Is Excellent Service

As the front end implements improved policies and processes to ensure accurate patient identification, patient education is a key component. Patient access employees should stress with patients that additional measures to verify their identity are being taken to protect them and their loved ones, from medical identity theft and to ensure patient safety.

To involve patients and patient families, the Joint Commission offers suggestions for health care providers to involve patients and patients' families in accurate patient identification. The Joint Commission recommends providers:

- Educate patients about the risk related to patient misidentification;
- Ask patients or their family members to verify identifying information to confirm that it is correct;
- Ask patients to identify themselves before receiving medical services and/or medications; and
- Encourage patients, patients' families, or their surrogates to be active participants in accurate patient identification, to express concerns about

patient safety, and to ask questions about the correctness of their medical care.

Technology Solutions

In addition to manual processes, the requirement of photo IDs and other proof of patient identity, health care providers may also tap technology to assist in accurate patient identification. Technology to verify a patient's identity includes use of fingerprint scanning technology, bar coding, and biometrics—among other technologies.

The Kramer Group (TKG) Healthcare Technologies, a national service provider of Registration Quality Improvement (RQi), is among the firms at work in combating medical identity theft. RQi is an automated, Web-based solution designed to detect and flag registration errors for correction prior to discharge and billing.⁶

The next generation release of TKG's custom service solution will empower patient access professionals with patient address and medical identity validation at the "front door." This new technology will provide front-end employees with the opportunity to triple check and validate a patient's information before receiving services—both in "real time" and overnight batch mode processing.

"This technology provides unparalleled accuracy at the time of patient registration, making it possible for easy, advanced checking and retrieval of vital registration information at the point of entry" notes Chuck Kramer, TKG Healthcare Technologies president and chief executive officer.

The new services will check for a basic postal service address deliverability match; a comprehensive address deliverability match, including national change of address (NCOA); plus Social Security, date of birth, and address validation cross-matches. The technology uses a patent-pending, state-of-the-art rules engine and a customized set of business rules that provides up to 100 percent data accuracy and improved employee accountability.

Another technology solution to combat medical identity theft is offered through HT Systems' PatientSecure. This system combats medical identity theft through biometric patient identification at the point of care.

PatientSecure prevents health care identity theft by creating a one-to-one match between a patient's biometric palm vein pattern and the patient's electronic health record. This biometric lock on the

patient's medical record makes it impossible for an imposter to impersonate a patient.

Whether medical identity theft is perpetrated by sophisticated criminals trying to commit health care fraud, or a patient using a stolen identity to obtain medical services they could not otherwise afford, PatientSecure is a tool that gives a health care provider organization the ability to combat medical identity theft directly.

In addition, PatientSecure crosses all platforms, even dissimilar systems. For instance, a patient enrolled at a specific hospital can be authenticated to any affiliated clinics or physician offices. Integrated within the health network's existing enterprise master person index (EMPI), electronic health records (EHR), and patient registration system, PatientSecure creates a blanket of identity protection over the entire network.

Along with preventing medical identity theft, PatientSecure also prevents the creation of duplicate health care records and accelerates patient registration times. The system also can identify an emergency patient who may be confused or unconscious, giving emergency department staff members their best chance at identifying a John or Jane Doe in seconds, which could save lives.

PatientSecure uses Fujitsu's portable PalmSecure, near-infrared light wave palm scanner to scan a patient's palm. This scan produces a unique biometric signature to that patient's unique vein pattern. It is 100 times more unique than a fingerprint

and more secure. This biometric signature is then attached to the patient's medical record and stored. By being portable, it gives the health care network the ability to scan patients in registration areas, waiting rooms, at the bedside, and in the emergency department.

PatientSecure is currently in use at Carolinas Healthcare, a health care system with 20 hospitals and 150 clinics. The system offers patients peace of mind in knowing that their health care identity is secure, which accounts for 98 percent patient participation and acceptance rate at the Carolinas facilities. ■

Notes

1. World Privacy Forum, "Medical Identity Theft: The Information Crime that Can Kill You," May 2006, available at http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf.
2. *Id.*
3. See <http://www.iom.edu/?id=12735>.
4. "Update: HIPAA Privacy and Security Rules," *Healthcare Registration*, April 2008, vol. 17, no. 7.
5. See http://www.jointcommission.org/patientsafety/nationalpatient_safetygoals/08_amb_npsgs.
6. "QA Makes a \$2.5 Million Difference: Assured registration accuracy speeds billing," *Healthcare Registration*, Nov. 2005, vol. 15, no. 2, p. 1.

Reader's Resource

For more information on The Kramer Group TKG Healthcare Technology Solutions' Registration Quality Improvement (RQi) system, visit the firm's Web site, at www.kramergroup.com. For more information on HT Systems' PatientSecure product, go to www.patientsecure.com.

Reprinted from *Employee Healthcare Registration*, June 2008, Volume 17, Number 9, pages 1, 8 to 11, with permission from Aspen Publishers, Inc., a Wolters Kluwer business, New York, NY, 1-800-638-8437, www.aspenpublishers.com.