



## Protecting Patient Identity

---



By David J. Gibson, MD

THE HEALTH CARE SYSTEM in the United States is under assault by organized crime. The reason - the system is the richest source of readily available cash in the economy. Health care consumes one in seven dollars and is growing at a rate six times greater than the rest of the economy.

Criminals attack the entire health care system, not just government entitlement programs. A total of \$85 billion, or 5 percent<sup>1</sup>, of the \$1.7 trillion in U.S. health care spending in 2003 was lost to health insurance fraud, according to the Blue Cross Blue Shield Association. That means fraud consumed all of a worker's contribution<sup>2</sup> to coverage during 2004.

Identity theft of information from the patient's medical record is the most common cardinal event in health care fraud. Unfortunately, one of the major sources from which criminals obtain this information is the physician's office. Given the access to personal information, a physician must take special precautions and have operating antifraud protocols in place to protect his or her patient's identifying information.

Medical Identity theft involves obtaining an individual's demographic and health insurance information, including Social Security number, without consent to commit claims fraud or other crimes. Criminals use a beneficiary's medical identity information to generate invoices for goods and services that are never delivered to the patient. This activity damages the beneficiary's personal health record and defrauds his or her plan. Criminals may also open fraudulent new accounts, forge checks in the beneficiary's name, transfer titles, generate money orders, and open bogus phone service accounts. They can even file bankruptcy, and often commit additional crimes, in the beneficiary's name.

Identity theft is a frequent occurrence. There are over 10 million victims of identity theft in the United States each year. On average, it takes 175 hours of work for victims of identity theft to clear their good name. In most cases, victims do not even know their identity has been stolen until they are denied employment or insurance coverage because of false health information placed in their medical records by a criminal's fraudulent transactions.

Overall, identity theft represents a \$47 billion dollar problem for America's economy and generally causes at least \$4,800 in losses for the defrauded individual. To put this problem into perspective, the following summarizes the likelihood that a beneficiary will be the victim of various types of crime:

Violent crime: <sup>3</sup> 1 in 5,000

Heart disease: <sup>4</sup> 1 in 2,600

Car accident: <sup>5</sup> 1 in 130

Identity theft:<sup>6</sup> 1 in 30

The reason criminals favor stealing a beneficiary's medical identity is understandable. With this information, they can obtain high-demand expensive aids, pharmaceutical products and other medical supplies that are easily fenced in the burgeoning gray market of wholesalers, or sold directly to other purchasers at a discount through the Internet.

The amount of confidential information demanded from beneficiaries before they can access the health care system exposes them to devastating risk when their identity is stolen. Compounding the problem, beneficiaries must routinely give all of their identifying demographic and financial information to each vendor of goods or services in the system. This information routinely includes not only name and address but birthdate, Social Security number, health insurance account numbers, and credit information including bank account numbers. Armed with this information, criminals can reconstruct and misuse an individual's identity.

This sensitive information is all too frequently obtained from medical offices where patient records are not effectively secured from temporary or low paid custodial staff members looking to supplement their incomes. Depending upon the market and the demographics of the source, this information's value on the street runs well above \$100 per stolen identity.

Physicians face a growing reality in the complex health care system of today. We must step forward and actively protect our patients from criminal activity in the industry.

Otherwise, patients face catastrophic complications ranging from personal financial ruin to inaccurate health care information within their medical records that can prove fatal. It is imperative that every medical office have operating systems in place that are regularly tested to protect the patient's identity.



When SSVMS Executive Director Bill Sandberg went out to lunch one day in October 1997, this was the last thing he expected to run across: a dumpster over-flowing with medical records from a clinic, now defunct. He reported it, photographed it and gave a statement to the court. And he has wondered many times about the potential misuse of those records had he not spotted them.

[djgibson@winfirst.com](mailto:djgibson@winfirst.com)

1. In *License To Steal* - Second Edition; Malcolm Sparrow, of Harvard University's John F. Kennedy School of Government, estimates the loss to be more than 15 percent in commercial insurance.
2. Both deductibles and co-payments.
3. 2000 U.S. Census.
4. *ibid.*
5. 2003 Bureau of Transportation Statistic.
6. 2003 Federal Trade Commission Survey.

Sierra Sacramento Valley Medical Society  
5380 Elvas Avenue #100 • Sacramento, CA 95819  
916.452.2671 PH • 916.452.2690 FX • Email: [info@ssvms.org](mailto:info@ssvms.org)

Copyright © 2000-2008 Sierra Sacramento Valley Medical Society - All Right's Reserved