

# ONCOLOGY TIMES

Publishing for **29** Years

[www.oncology-times.com](http://www.oncology-times.com)

Lippincott Williams & Wilkins  
Wolters Kluwer Health

THE **NEWS CENTER** FOR THE CANCER CARE TEAM

## Medical Identity Theft: More Common than Generally Known, Cancer Patients Among the Most Vulnerable

Page 8



Photo collage by Vincent Ciarrano

### From the Chemotherapy Foundation Symposium:

(1) CLL: Oblimersen + Chemotherapy Improves Outcome; (2) Judah Folkman Update on Antiangiogenic Drugs; (3) Satraplatin on Fast Track for Approval for Hormone-Refractory Prostate Cancer; (4) Pancreatic Cancer: Gemcitabine Oxaliplatin Doublet OK for Induction; (5) Tumors of Unknown Origin: Microarray Assay Reliably Identifies Primary Site in Early Testing; (6) Gastroesophageal Cancer: Refining Use of Targeted Agents; (7) Lung Cancer & Platinum Regimens; (8) Obatoclax for Hematologic Cancers

Pages 30, 38, 39, 43, 46, 49, 50, 58



**HYPER-THERMIC IP CEMO-THERAPY**

**Advanced Colorectal Cancer: Consensus Group Advises**

**Heated Post-Surgery Chemo, but Others Disagree, Citing Lack of Phase III Data**

Page 24

### Pay for Performance: NCQA Says It's *an* Answer, Not *the* Answer

Page 6



### Eric Rosenthal on New Academic-Industrial Alliances

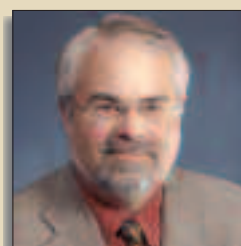
Page 19



### SIMONE'S ONCOPINION: Mourning and Grieving for Chris

NCCN Medical Director Christopher E. Desch, MD, Killed in Plane Crash

Page 2



- No Extension for CMS Demo Project ..... 7
- PSA Bounce Does Not Signal Higher Mortality, Recurrence Risk ..... 15
- NSCLC: Adding RT Extends Survival Time for N2 Patients ..... 29
- Web Tool Can Help Guide Use of Radiation in Breast Cancer ..... 36
- Lung Cancer: 3D RT Superior to 2D for Inoperable Patients ..... 42
- Stabilizing Bone after Vertebral Fracture Leaves Room for Meds ..... 55
- RT Boost in Early Breast Cancer Does Not Extend Survival ..... 56



**ScriptDoctor: Medicine in the Media**

Fact-checking Fiction

Page 52

### DEPARTMENTS

LETTERS

POETRY BY CAREGIVERS

EYE ON WASHINGTON

SHOP TALK

**H NEWS CENTER**  
M U  
A T O L O N C O L O G Y  
P H A R M A C Y  
S I N

# Medical Identity Theft: Under-reported, Under-researched, & More Common than Generally Known

## *Cancer Patients Among the Most Vulnerable*

By Margot J. Fromer

**M**edical identity theft is stealing health information for personal profit. If that sounds like a strange thing to do, it is, but it is more common than generally thought. What is known about it remains sketchy because it is the most poorly documented of all identity theft crimes, according to the Federal Trade Commission (FTC), which estimates that approximately 250,000 to 500,000 people have been victimized since the agency starting tracking the crime in 1992 and that the real number could be three times that.

The FTC speculates that 1.5% of all Americans are victims of medical identity theft each year, and the crime increased almost 200% between 2001 and 2005.

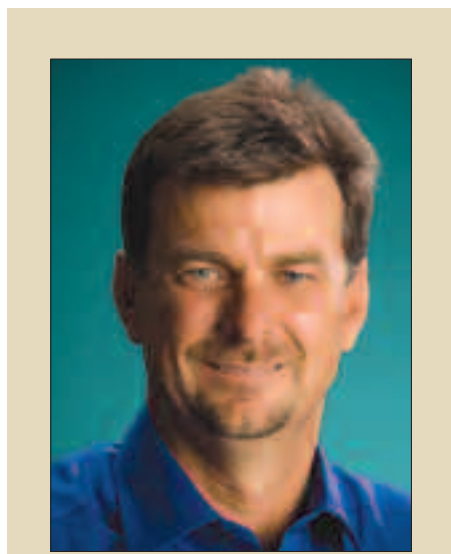
Kurt Long, CEO of EpicTide, a company in St. Petersburg, FL, that markets corporate security, told *OT* that there are probably a half million victims to date, a number that will probably increase now to be 250,000 each year.

*Medical identity theft is the most poorly documented of all identity theft crimes.*

Here's how it works: A thief uses a victim's name and/or other identifying information without the person's knowledge or consent to obtain medical services. Or, the thief uses the stolen data to make false claims for medical services. The victim, or the insurance company, is billed for services not received. Even more frightening, the victim can end up with false information entered on his or her medical record, or an entirely new fictitious medical record is created.

It can be notoriously difficult to uncover, according to a report last May by the World Privacy Forum (WPF), a nonprofit, public-interest research group in Cardiff, California, that describes itself as focusing in a nonpartisan way on research and consumer education in the intersecting areas of technology and a range of privacy matters, including financial, medical, employment, and Internet privacy.

"Medical identity is well hidden in large electronic payment systems and in widely dispersed databases and medical files," the report (titled "Medical Identity Theft: The Information Crime that Can Kill You") notes. "Medical identity thieves are usually professionals adept at making sure vic-



**Kurt Long, CEO of a company in Florida that markets corporate security: "The thieves get away with it because there are no big fines, no jail time, and no enforcement of the existing weak regulations....We need to devise a multiplicity of solutions: physical security of medical data, photo ID at the point where care is provided, and automated auditing of medical records....Until there are strong laws, accompanied by strong enforcement and effective technology, things are unlikely to improve."**

tims do not detect the crime—ever."

Organized crime rings are heavily involved, often in collusion with health care employees such as office and medical records personnel and insurance claims clerks. "These rings are very organized and highly sophisticated, and they depend heavily on insiders," the author of the report, Pam Dixon, the organization's Executive Director, told *OT*.

The four most vulnerable types of patients are those with cancer, diabetes, and AIDS, and those who are residents of inpatient drug treatment centers.

Occasionally the crime is more "innocuous," Ms. Dixon continued. A poor person without health insurance needs medical care and believes the

only way to get it is to steal it. Or someone lifts a wallet at a mall and finds a health insurance card among the other treasures.

### How Victims Are Harmed

Victims of medical identity theft learn about the crime in various ways: through a collection notice for bills they did not incur, an erroneous entry on a credit report, denial of insurance or notification that a payout cap has been reached, or irregularities in health insurance explanation of benefits (which most people don't bother to read or can't understand).

In addition, they may be denied employment because someone else's illness is on their record, or receive the wrong medical treatment because of erroneous information in their own file—a situation that is particularly dangerous in the emergency department.

Imagine a bleeding patient given a transfusion of the wrong type blood. Or someone with a hot gallbladder told he had it removed two years ago. Or a cancer patient's file that has someone else's PET scan.

Or erased data about a previous anaphylactic reaction to penicillin.

And what if the thief has died, but the victim is still alive and needs medical care? Think about walking into a doctor's office (or worse, the ER) and being informed that you're dead.

Use of stolen medical information is rarely a one-shot deal. The FTC says that it is often misused for "a substantial period of time." Thirteen percent of victims report misuse for six months or more.

### Victims Almost Powerless

Victims of medical identity theft cannot escape the consequences because they have no enforceable rights, Ms. Dixon

noted. Patients can see their medical records (usually after asking more than once and having to pay for a photocopy), but they cannot correct errors, and the theft may not even be evident in the record.

Moreover, they are powerless to prevent providers, clearinghouses, and insurers from perpetuating the fraudulent information.

Ms. Dixon said that victims do not have the legal right to demand correction of medical information that was not created by the provider or insurer currently using it—even when false entries were put in the record during commission of a crime.

Health care providers are not required to amend records they didn't create, and they are reluctant to do so voluntarily for fear of liability. So victims of medical identity theft can spend years running from doctor to doctor, to insurance company, to laboratory, to pharmacy trying to get things straightened out. In the end, mistakes keep slipping by.

*The types of patients most vulnerable to identify theft are those with cancer, diabetes, and AIDS, and those who are residents of inpatient drug treatment centers.*

"Nightmarish" is the word one hears most often in connection with medical identity theft, Ms. Dixon said. Because there are no laws, there is no one to call for help. The crime should be reported to local police, but that is usually futile, and if the victim notifies anyone else, he or she may be reporting the crime to the same people who committed it.

One of the big problems, according to the WPF report, is that victims fall through law enforcement gaps—chasms, really—because no one agency knows how to help.

For example, financial identity theft experts know little about medical affairs or the complexities of the Health Insurance Portability and Accountability Act (HIPAA). The FTC is not responsible for medical issues, and the Department of Health and Human Services has no published studies or guidance about medical identity theft, which is not the same as health care fraud.

*Victims of medical identity theft cannot escape the consequences because they have no enforceable rights. Patients can see their medical records (usually after asking more than once and having to pay for a photocopy), but they cannot correct errors, and the theft may not even be evident in the record. Moreover, victims are powerless to prevent providers, clearinghouses, and insurers from perpetuating the fraudulent information.*

(continued on page 11)



## EYE ON WASHINGTON

### ■ CMS Hospital OPD Rule for 2007

The final rule of the Centers for Medicare & Medicaid Services (CMS) for Medicare payments for hospital outpatient services for this year is designed to make payments more accurate and promote higher quality and value in outpatient care, a statement from the agency said. Included in the outpatient prospective payment system (OPPS) are provisions for expanding quality reporting requirements, as well as the list of services for which Medicare will make payment to ambulatory surgical centers.

The Ambulatory Payment Classification payment and coding structure for drug administration services was revised, allowing hospitals to report the

same CPT codes for drug administration used by physicians and other payers, and allowing separate payment for additional hours of infusion. As a result, hospitals should be paid more accurately for complex and lengthy drug administration services.

Medicare will pay for drugs and biologicals at 106% of the average sales price (ASP). Radiopharmaceuticals will be paid at charges adjusted to cost, using hospital-specific cost-to-charge ratios. Payments for other drugs will continue to be bundled into payments for their associated procedures. CMS also will pay separately for drugs, biologicals, radiopharmaceuticals, and anti-nausea drugs that cost \$55 or more per day.

Other provisions of the final rule are that:

- Beginning in 2009, OPPS rate increases will be tied to reporting of quality measures.

- Per diem payment for partial hospitalization services will be reduced by 5% (instead of the proposed 15%) in 2007.

- Administering hospital claims for outpatient services will be gradually changed from fiscal intermediaries and carriers to the new Medicare Administrative Contractors.

- Nineteen procedures will be added to ambulatory surgical centers.

The Association of Community Cancer Centers issued a news release in support of the new plan: "ACCC worked very hard with Congress and with CMS to keep 2007 drug reimbursement no lower than the 2006 levels, Executive Director Christian

Downs, JD, said. "By keeping the payment rate at ASP plus 6%, CMS has chosen to protect cancer patients' access to quality care."

The Association is still concerned, though, Mr. Downs said, that CMS has chosen not to reimburse hospitals for pharmacy and acquisition costs because, said CMS, these costs are included in charges for drugs.

### ■ CMS Physician Fee Schedule for 2007

Medicare payments to physicians will be cut by 5% this year under the physician fee schedule issued by CMS. The cut is a slight change from the 5.1% reduction calculated when the rule was *(continued on page 14)*

## Medical Identity

*continued from page 8*

Mr. Long called health care organizations particularly vulnerable, saying that some employees are induced to provide rosters of patient names to crime rings. Moreover, partly because of HIPAA as well as other circumstances, "the thieves get away with it because there are no big fines, no jail time, and no enforcement of the existing weak regulations," he said.

*Financial identity theft experts know little about medical affairs or the complexities of HIPAA. The FTC is not responsible for medical issues, and the Department of Health and Human Services has no published studies or guidance about medical identity theft, which is not the same as health care fraud.*

### Electronic Exacerbation

Medical identity theft is relatively easy to commit now and will become easier as paper-based records are changed to electronic ones via the National Health Information Network and disseminated

to huge numbers of people who may or may not have legitimate access to them.

Current policy maintains that digitizing medical records will improve care, reduce fraud and errors, and save lives. This can be true, but committing private and sensitive data to cyberspace is an open invitation to steal, Ms. Dixon maintained.

"The more digitized the health care system becomes—and there's no stopping now—the greater the problem of medical identity theft. There's too much cheerleading about electronic records on the part of government administrators, insurance companies, and others, and not nearly enough emphasis on its downside: what it does to patients whose data are stolen. I don't know of any electronic program that has had risk-assessment studies prior to implementation."

Ms. Dixon said that she is not opposed to electronic records—"although paper does protect people—but if there was a risk-management process in place, things might be okay. Making the system hack-proof is a daunting task, but it must be done."

### Little Recourse—So Far

The World Privacy Forum report notes that identity theft is "deeply entrenched in the health care system," and that victims ought to have recourse in the form of a right to correct errors, remove false information, and receive one free copy of their medical record each year. Patients also should be informed of breaches in their records as soon as they occur.

The report recommended that:

- Studies be conducted to determine the incidence and nature of the crime in order to prevent and counteract it.

- Patients have expanded rights to their own health information in its various medical and financial forms.

- Patients should be informed about errors and allowed to correct them—in all iterations of the record.

- When patients have been victimized, they should have adequate legal and monetary recourse—equal at least to the protections offered to victims of financial identity theft.

In addition, public and private health insurers should send each beneficiary a free annual listing of all paid claims.

Mr. Long agreed: "We need to

devise a multiplicity of solutions: physical security of medical data, photo ID at the point where care is provided, and automated auditing of medical records."

He noted that some doctor's offices, hospitals, and HMOs have begun to ask patients for identification such as a driver's license or Social Security number. Still, considering how easy it is to buy a fake license, this isn't much extra protection.

Until there are strong laws, accompanied by strong enforcement and effective technology, Mr. Long said, things are unlikely to improve.

## Survey

A survey commissioned by Kurt Long's company, EpicTide, conducted in November, revealed that, despite increasing media reports, the public has little appreciation of how widespread and dangerous medical identity theft is.

The survey sought to find out if consumers are aware of the phenomenon, what the incidence is, how well they understand their rights before and after they have been victimized, and how well the health care system protects their records and ensures their safety.

Among the findings:

- Nearly half of respondents had never heard of medical identity theft and were mostly unaware of its serious consequences.

- But when the consequences were described, consumers' top three fears were the risk to life and health, loss of privacy and confiden-

tiality, and changes in their medical records.

- Several respondents had been victimized, and the majority had yet to resolve all the ensuing problems.

- The majority of victims did not know the perpetrator, but 18% of them had been victimized by a family member.

- Consumers are confused about privacy rights, and only 53% had been asked to sign a HIPAA notice at the point of medical service (most didn't read it).

- Respondents believe almost unanimously that health care providers and organizations are responsible for protecting their medical privacy, but only 40% think that this is being done.

- Even fewer—only 30%—believe that hospitals inform potential victims of suspected breaches of medical record security.