

Health Care Compliance LETTER

Volume 11, Issue 12

health.cch.com

June 10, 2008

On The Front Lines 4

Medical identity theft: Patient access first in line to manage the nation's fastest growing crime

by **Laura J. Merisalo,**
Contributing Editor

Tax-Exempt Organizations 1

- Revised Form 990 may be “audit road map,” expert says
- IRS EO officials discuss hospital questionnaires

Medicaid 2

- Medicaid regulations will impede trauma care, Waxman warns

Antitrust 7

- Court affirms price-fixing determination against physician group

Fraud and Abuse 8

- Pharmacy chain settles Medicaid fraud claims

In The News 8

Revised Form 990 may be “audit road map,” expert says

Revised Form 990, Return of Organization Exempt from Income Tax, touted by the Internal Revenue Service (IRS) as increasing transparency in the nonprofit sector, also may be an “audit road map,” Joseph A. Rieser, Partner, Arent Fox, LLP, told nonprofit professionals at an April 3, 2008, program presented by Arent Fox and the Reznick Group in Washington, D.C. He called the level of detail now required by the IRS on Form 990 “striking.”

Executive compensation. Nonprofit executive compensation is a “hot button” issue, Rieser said, and many of the questions about compensation on the new Form 990 reflect recent reports of abuses. Nonprofits must report first-class or charter travel, travel for companions, discretionary spending accounts, personal services, and payments for business use of a personal residence. “If you check one of these boxes, you can be sure to expect further inquiry from the IRS,” Rieser predicted.

Good governance. “Revised Form 990 also reflects the [IRS] mindset that good governance is furthering the organization’s exempt purpose,” Deanne M. Ottaviano, Partner, Arent Fox, said. Ottaviano and Anne Schrantz, Principal, Reznick Group, described a checklist of corporate governance questions on the new Form 990. They include whether the exempt organization’s board: (1) reviewed the Form 990 before filing; (2) has a written conflict-of-interest policy; and (3) contemporaneously documented board and committee meetings.

The questions take you to the answers the IRS wants, Schrantz cautioned. Question 5 in Part VI, for example, asks, “Did the organization become aware during the year of a material diversion of the organization’s assets?” Essentially, this question is asking, “Was there any fraud?” Schrantz explained.

The IRS also wants to know if the exempt organization invested in, contributed assets to, or participated in a joint venture with a taxable entity. “Few nonprofits have written policies on joint ventures and they will have to develop them,” Ottaviano noted. A joint venture policy must permit the exempt organization, among other things, to act exclusively in furtherance of its exempt purpose and only incidentally for the benefit of the for-profit entity.

Schedules. The revised Form 990 includes 15 schedules. The “core” of the new form contains “built-in triggers” that alert filers if they need to complete a schedule, John Salbergo, Tax Senior Manager, Reznick Group, explained. All nonprofits must complete the core form, but not every exempt organization will have to complete a schedule; for example, Schedule H is just for hospitals, Salbergo noted.

Instructions. Although the IRS released the revised Form 990 in 2007, “we are still waiting on final instructions,” Salbergo said. The IRS originally predicted that

Tax-Exempt Organizations (cont.)

it would issue final instructions in early 2008. It released draft instructions in early April and anticipates publishing the final instructions by the end of 2008.

CCH Exempt Organizations Reports, Issue No. 406, Report 406, May 12, 2008.

IRS EO officials discuss hospital questionnaires

The goal of the IRS Exempt Organization (EO) Division's hospital compliance project is to provide the IRS with a better picture of how tax-exempt hospitals operate, according to Geoffrey Campbell, IRS Tax-Exempt/Government Entities (TE/GE) tax law specialist. Campbell spoke at the American Bar Association Section of Taxation meeting on May 9, 2008, in Washington, D.C.

Objectives. Two objectives of the hospital project were to look at community benefit and executive compensation. The IRS sent out 544 questionnaires to hospitals in 2007, and over 99 percent responded. "Was it fear? Who knows? We didn't bribe them. We may have threatened them," Campbell joked. The final report is scheduled to be released in September.

Community benefit. Campbell said that the IRS pulled some census data information on where the hospitals are located. "It's hard to define the 'community' for purposes of the community benefit standard. The best way to do demographic analysis that we could come up with was based on county. That's imprecise because some counties are huge and hospitals overlap counties, but that's the best way we could think of."

According to Campbell, the IRS pulled per capita data information from the zip code where the hospital is located, along with levels of health care coverage. "There is one notable thing that we found looking at the demographic data analysis. You would expect where there is [a] higher level of uninsured there would be higher level of community benefit. That's what we found."

He continued, "But you would also expect that where the per-capita income was lower, you would find a higher level [of community benefit], but we didn't.

Per-capita income goes up, community benefit goes up. Health care coverage goes down, community benefit goes up. One possible explanation is that, in a really poor area, they have Medicare, and that is considered insured for purposes of the report. But we're still looking at that."

Executive compensation. The final report also will focus on compensation practices. Twenty exams in this area, based on excess compensation, are slowly wrapping up, Campbell said. Discussion of the exams will be included in the September report.

"We did not go into this project with an intent to change the Revenue Ruling 69-545 [1969-2 CB 117] standard [related to whether a nonprofit hospital claiming exemption under Internal Revenue Code §501(c)(3) is operated to serve a public rather than a private interest]. After the report is done and we get a couple years of reporting on Schedule H, we'll have information to provide lawmakers should they wish to go forward and change it," Campbell noted.

Commensurate doctrine. The commensurate test of Revenue Ruling 64-182, 1964-1 CB 186, generally measures if a charity is undertaking, through contributions and grants, a charitable purpose commensurate in scope with its financial resources. Lois Lerner, Director of the IRS EO Office, followed up on remarks about the test made by Steven Miller, Commissioner of the IRS TE/GE Division, at an earlier conference. "The revenue ruling is very old. We're going to be looking at it to see if it still applies to today's sector and marketplace," Miller said.

Lerner added, "This is not just a hot topic in the United States, but this is being discussed by other charity regulators in the English-speaking world. The Canadians have gone so far as to pass legislation that says, if a charity receives contributions in year one, it has to spend 80 percent of those contributions in year two. It's pretty strong stuff; we aren't there yet."

Voluntary compliance program. Lerner also said that the EO Division is developing a voluntary compliance program for nonfilers. "It is slower going than we hoped for," she noted. "If this voluntary compliance program works, we hope to

expand on it. The IRS Employee Plan Division has a voluntary reporting program. We want to get there as well, but we need to take baby steps to get there."

The IRS needs to coordinate this type of project all the way up the chain at the IRS and the Treasury, Lerner stated. Currently, the IRS is looking at the very narrow area of out-of-compliance organizations with regard to filing their Form 990s. The project would allow them to file all of their reports and get



Portfolio Managing Editor
Pamela K. Carron, J.D., LL.M.

Coordinating Editors
Susan Smith, J.D., M.A.
Valerie Witmer, J.D.

CCH Washington Bureau
Paula Cruickshank
DOJ, FTC—John Scorza
SEC—Peter Feltman

Health Law—Catherine Hubbard, M.A.
Tax—Jeff Carlson, Steve Cooper,
Chandra Walker, George L. Yaksick, Jr.

CCH Tax-Exempt Advisor
Larry Perlman, CPA, JD, LL.M.

Designer
Biren Patel

Requests for information about article submission and comments from readers are welcome and should be directed to Susan Smith at susan.smith@wolterskluwer.com, Tel. 847-267-2780, Fax 847-267-2514. Customer service inquiries should be directed to 800-449-9525.

CCH Health Care Compliance Letter is published 24 times a year by CCH, a Wolters Kluwer business, 4025 W. Peterson Avenue, Chicago, IL, 60646. Subscription rate is \$305 per year. First-class postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: SEND ADDRESS CHANGES TO *CCH Health Care Compliance Letter*, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A. ©2008 CCH. All rights reserved.

No claim is made to original government works; however, the gathering, compilation, and arrangement of such materials, the historical, statutory and other notes and references, as well as commentary and materials in this Product or Publication are subject to CCH's copyright.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting or other professional service. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

For more information about the CCH Health Care Compliance Portfolio, please visit our online store at <http://health.cch.com>.

Tax-Exempt Organizations (cont.)

them in compliance so they can go forward and not have to worry about their exemption. "I think having a broader voluntary compliance program is the way to go."

Governance. "We understand that governance is not [within the] purview of the IRS," Lerner explained. "We will use our bully pulpit to talk about governance. We know that the states are very involved in this, that their jurisdiction covers this. We're working with the states. Our idea is not to take over from the states, but to

assist the states and sector."

Lerner also said, "We're at the baby stage here. But we will keep going in this area, I think, to try to leverage governance-enhanced compliance and transparency through accountability, and to help organizations move through the process with the IRS, both in determination and examinations." She said that IRS agents will be trained so that "you don't have to have a specific 'thing' to get past our process."

Education. The IRS EO Customer

Education and Outreach Division is working on making podcasts available for download, Lerner reported, "so that while you're exercising, you can listen on your iPod to your EO training sessions." Subjects of the podcasts will include: foundation classifications; deduction of charitable contributions; political campaigns and charities; and navigation of online resources for tax-exempt organizations. ■

CCH Exempt Organizations Reports, Issue No. 407, Report 407, June 9, 2008.

Medicaid

Medicaid regulations will impede trauma care, Waxman warns

Pending cuts in Medicaid payments to hospitals will hamper hospitals' ability to care for injured people in the event of a major catastrophe, such as a terrorist attack, according to House Oversight and Government Reform Committee Chairman Henry Waxman (D-Calif.), who held two hearings on the subject in early May.

The committee also released the results of a recent survey showing that hospitals in seven cities lack sufficient emergency care capacity to respond to an attack the size of one that occurred in Madrid, where nearly 1,000 people needed treatment.

ED overcrowding. Waxman said the nation's emergency departments (EDs) already are operating at or over capacity, adding that if the nation does not address the chronic overcrowding of emergency rooms, their ability to respond to a public health disaster or terrorist attack will be severely jeopardized.

A survey of 34 Level I trauma centers, which included facilities in New York City, Los Angeles, Washington, D.C., Chicago, Houston, Denver, and Minneapolis, revealed that the hospitals: (1) did not have sufficient ED capacity to treat a sudden influx of victims from a terrorist bombing; (2) had virtually no open intensive care unit beds to treat the most seriously injured casualties; and (3) did not have enough regular inpatient beds to handle the less seriously injured victims.

Criticism of HHS regulations.

HHS has issued three Medicaid regulations that will reduce federal funds to public and teaching hospitals by tens of billions of dollars over the next five years, Waxman said. "It appears that [HHS] Secretary [Michael] Leavitt signed regulations that will take hundreds of millions of dollars away from hospital emergency rooms without once considering the impact on national preparedness," he said.

The earliest cuts would begin May 26, 2008. The House has voted to postpone implementation until April 1, 2009, to review the regulations.

HHS response. Leavitt said that while hospital capacity for surges is not

where HHS would like it to be, the regulations will ensure that states are paying their fair share. He explained that hospitals have been taking federal dollars for patient care and putting them in general funds. The regulations will ensure the funds are used to treat patients, he said. "This isn't about trauma centers, it's about the relationship between the states and the national government."

If Congress determines there is a need for additional dollars to improve hospital surge capacity, HHS can direct more funds to the hospitals, Leavitt said. Waxman said that the "tiny grants" to hospitals have not been enough to improve surge capacity. ■

CCH Washington Bureau, May 8, 2008.

CCH Health Care Compliance Editorial Advisory Board

Timothy P. Blanchard, Esq.
McDermott Will & Emery

Patricia L. Brent, J.D., M.P.H.
President, Morgan Hill Associates

Michael E. Clark, J.D., LL.M.
Partner, Hamel Bowers & Clark LLP

Bill Dacey, MBA, MHA, CPC
President, The Dacey Group

Allan P. DeKaye, MBA, FHFMA
DeKaye Consulting, Inc.

Paul R. DeMuro, J.D., MBA
Partner, Latham & Watkins

Albert Y. Lin, Esq.
Partner, Brown McCarroll, LLP

Jeffrey B. Miller, Esq.
Chief Compliance Officer, Synthes Inc.

Stephen A. Miller, J.D.
Chief Compliance Officer, Capital Health System

Corrine Parver, J.D.
American University College of Law, Washington, D.C.

Cynthia Reaves, Esq.
Deloitte Services LP

Fay A. Rozovsky, J.D., M.P.H.
President, Rozovsky Group

William P. Schurgin, Esq.
Seyfarth, Shaw, Fairweather & Geraldson

John E. Steiner, Jr., Esq.
*Chief Compliance Officer,
UK HealthCare of Lexington, Kentucky*

Sanford V. Teplitzky, Esq.
Ober, Kaler, Grimes & Shriver

Medical identity theft: Patient access first in line to manage the nation's fastest growing crime

by Laura J. Merisalo, Contributing Editor

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 occurs 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 by sophisticated criminals. When medical identity theft is perpetrated by sophisticated criminals, it generally is the first step in a larger scheme to commit health care fraud for financial gain. Perpetrators steal patient identities and then buy, sell, or use those identities to submit false claims for payment for medical services to treat 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 to receive 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, while 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 threatening 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 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 associated with 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 (indeed, it 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 can go 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 identity 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 privacy also are hot button health care issues, which are further exacerbated by this crime.

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 may 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 a medical identity 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 implementation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security rules.⁴ As it turns out, HIPAA is not a panacea to protect patients' private and personal health care information, particularly as the health care industry increasingly relies upon electronic health records for clinical and administrative functions. It is difficult, if not impossible, to guarantee that improper access to and fraudulent use of such privileged information is avoided.

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 organizations can take to verify patient identities—to ensure patient safety and avert health care fraud. The onus is on providers to protect the people they serve, particularly because 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 that they receive quality health care.

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.⁵

The Joint Commission offers the following suggestions to improve accurate patient identification:

- Emphasize to employees that a significant 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.
- Educate patients on the importance and relevance of correct patient identification in a positive fashion that also respects concerns for privacy.

Photo ID as 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, where the patient's photo ID is scanned into the system. If a patient presents for care without a photo ID and does not have a photo ID already scanned into the system, front-end employees take the patient's picture (provided he or she is over the age of 18 or emancipated) to enter into the system. This helps verify patient identity, ensure patient safety, and improve accurate patient account identification.

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

Patient involvement in identification

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 ensure patient safety.

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

- educate patients about the risks related to patient mis-identification;
- ask patients or their family members to verify identifying information;
- ask patients to identify themselves before receiving medical services or medications; and
- encourage patients, patient families, or their surrogates to be active participants in accurate patient identification, express concerns about patient safety, and ask questions about the appropriateness of their medical care.

Technology solutions

In addition to manual processes and the requirement of photo

IDs and other proof of patient identity, health care providers also may tap technology to assist in accurate patient identification. Technology used to verify a patient's identity includes fingerprint scanning technology, bar coding, and biometrics, among other tools.

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—both in "real time" and through overnight batch mode processing—before services are provided.

The new services will check for a basic postal service address deliverability match; a comprehensive address deliverability match,

including national change of address; and Social Security number, date of birth, and address validation cross-matches. The technology uses a patent-pending, state-of-the-art rules engine and customized set of business rules that provide up to 100 percent data accuracy and improved employee accountability.

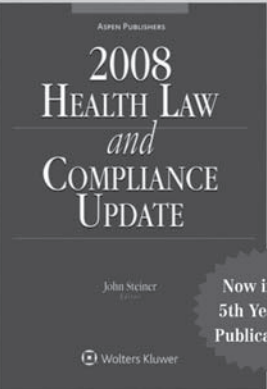
Another technology solution to combat medical identity theft is offered through HT Systems' PatientSecure. This system combats medical identity theft through biometric patient identification at the point of care.

PatientSecure prevents medical identity theft by creating a one-to-one match between a patient's biometric palm vein pattern and electronic health record. This biometric lock on the patient's medical record makes it impossible for an imposter to impersonate a patient.

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, electronic health records, 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

2008 Health Law and Compliance Update



Now in its
5th Year of
Publication!

ISBN: 9780735566316, \$229.
Softcover, Published Annually

The 2008 Edition of *Health Law and Compliance Update* brings you the latest information on emerging issues in health law and health care compliance. Each chapter is authored by experts from some of the most prestigious law and consulting firms, including McDermott Will & Emery; Holland & Knight; Davis Wright Tremaine; Manatt, Phelps & Phillips; Broad and Cassel; Huron Consulting; and PriceWaterhouseCoopers.

Health Law and Compliance Update includes in-depth analysis of such topics as

- Electronic Medical Records Legal Issues
- Antitrust in Evolving Provider and Payor Markets
- Medicare Part D Compliance
- Clinical Research Billing
- Compliance and Governance for Health Care Organizations
- And more!

Also, the 2008 Edition also provides a variety of tools, diagrams, and other easy-to-use reference tools including:

- Health Information Management Processes Examined During JCAHO Evaluation
- Additional Coding and Billing Requirements for Clinical Trials
- Definitions for the Coding Terminology
- Broken Charge Cycle Diagram
- Part D Oversight Strategy Diagram

SUMMARY OF CONTENTS

1. Year in Review
2. Comprehensive Analysis of the Basis for Compliance and Governance for Health Care Organizations
3. Antitrust in Evolving and Consolidating Provider and Payer Markets
4. Medicare Part D Compliance
5. Equity Transactions in the ASC Industry
6. Things You Need to Know in Charging for Hospital and Physician Services
7. The New Breed of Hospital-Physician Collaborations: Is Government Backlash Around the Corner?
8. Billing Compliance in Clinical Research
9. Legal Implications for Electronic Medical Records
10. Using Microsoft Access to Create an Arrangements Database: iFAQs.

Wolters Kluwer | Aspen Publishers
Law & Business

Aspen Publishers is now part of Wolters Kluwer Law & Business.

Call 1-800-638-8437 or visit www.aspenpublishers.com
to order your 30-Day RISK-FREE copy!
(Refer to Priority Code AA09)

an emergency patient that 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 based on that patient's unique vein pattern. It is 100 times more unique than a fingerprint and more secure. This biometric signature then is attached to the patient's medical record and stored. Its portability gives the health care network the ability to scan patients in registration areas, in 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. ■

Laura J. Merisalo is editor and principal author of *Healthcare Registration*, a national newsletter for patient access professionals. Ms. Merisalo also is associate editor for a newsletter on legal issues related to health care reimbursement, contributing editor for a quarterly analysis of hospital accounts receivable, and consulting editor for a comprehensive health care registration manual. She has served as a contributing author for books and manuals on patient access services and health care revenue cycle management processes. Ms. Merisalo can be reached at hcr@wi.rr.com.

* Reprinted from HEALTHCARE REGISTRATION, Vol. 17, No. 9, June 2008.

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, Vol. 17, No. 7, April 2008.

⁵ See http://www.jointcommission.org/patientsafety/nationalpatientsafetygoals/08_amb_npsgs.

⁶ "QA Makes a \$2.5 Million Difference: Assured registration accuracy speeds billing," HEALTHCARE REGISTRATION, Vol. 15, No. 2, Nov. 2005.

Antitrust

Court affirms price-fixing determination against physician group

The Federal Trade Commission's (FTC's) determination that a physician group's activities with respect to its fee-for-service, or nonrisk, arrangements with payors constituted horizontal price-fixing unrelated to any procompetitive efficiencies was supported by substantial evidence, according to the Fifth Circuit Court of Appeals. The FTC correctly found that the physician group, North Texas Specialty Physicians (NTSP), violated the antitrust laws by collectively negotiating with health plans on behalf of its member physicians in an attempt to obtain higher fees.

The FTC's remedial order, however, was overly broad because it could have the effect of compelling NTSP to negotiate or enter into contracts with payors, regardless of the potential risks to NTSP, its physicians, or its patients, the court concluded. Therefore, NTSP's request for review of the FTC's order was granted, and the case was remanded to the FTC for modification of the remedial order only.

Nonrisk contracts. When NTSP negotiated its nonrisk contracts with health insurers on behalf of its members, it first polled the physicians to determine the minimum fee they would accept for

medical services provided under a group payor agreement. NTSP then reported to its participating physicians the results of these polls and, based on the poll calculations, calculated a minimum contract fee that it used to negotiate managed care contracts.

NTSP would "messenger" the offers it received from payors to the member physicians, who would then decide whether to accept or reject the offers. The physicians had limited exclusivity with NTSP, such that they could deal with a payor only if NTSP was not negotiating with that payor or the agreement between NTSP and the payor did not cover the services that the physicians sought to provide.

FTC decision. The FTC issued an administrative complaint charging NTSP with unlawfully restraining competition through horizontal price-fixing in violation of §5 of the FTC Act. An FTC administrative law judge upheld the complaint and entered a cease and desist order that, among other provisions, required termination of existing nonrisk contracts at the payor's request or at the earliest termination or renewal date.

Appeal. NTSP made several arguments on appeal, which the Fifth Circuit addressed in turn. First, the court concluded, the FTC had jurisdiction because, if NTSP's attempts to maintain physicians' fees were successful, competition would be adversely affected. Second, NTSP's activity

with respect to its nonrisk contracts constituted concerted action because NTSP was controlled by competing physicians and, therefore, was not a sole actor for purposes of the antitrust laws.

Third, an abbreviated "inherently suspect," or "quick-look," analysis, rather than a full rule-of-reason analysis, was appropriate because the anticompetitive effects of NTSP's activities were obvious and the procompetitive justifications did not plausibly result in a net procompetitive or neutral effect on competition, the court found.

Finally, as to the merits of the alleged violation, the court determined that substantial evidence supported the FTC's findings that NTSP's activities constituted horizontal price-fixing and, accordingly, affirmed the FTC's determination. The court stated that NTSP: (1) actively encouraged physicians to reject offers from that fell below the fees indicated in the polls; (2) delayed or blocked direct negotiations between payors and physicians in an attempt to increase its collective bargaining power; and (3) engaged in contract negotiating practices that resulted in contracts that contained fees higher than many participating physicians otherwise would have been willing to accept. ■

North Texas Specialty Physicians v. FTC, 5th Cir., May 14, 2008, *Health Care Compliance Reporter* ¶1800,510.

Fraud & Abuse

Pharmacy chain settles Medicaid fraud claims

Walgreen Co. (“Walgreens”), a national chain of retail pharmacies, has agreed to pay the U.S., 42 states, and Puerto Rico \$35 million to settle allegations of Medicaid prescription drug fraud, state and federal officials announced. The settlement resolves claims initiated by a whistleblower who alleged that Walgreens substituted different versions of prescribed drugs solely to increase its reimbursement rate.

From 2001 to 2005, Walgreens allegedly dispensed to Medicaid patients more expensive versions of Ranitidine, Fluoxetine, and Eldepryl than were prescribed. Its pharmacies replaced doses of Fluoxetine, prescribed in capsule form, with more expensive tablets. Ranitidine and Eldepryl, prescribed in tablet form, were replaced with capsules reimbursed at a higher rate.

According to a press release issued by the U.S. Attorney, Northern District of Illinois, “While capsules and tablets generally function in the same way when they enter the body, both federal Food and Drug Administration law and state statutes provide that the different dosage forms of the same compound are not considered the same. Therefore, pharmacists cannot switch customers between capsule and tablet forms of a medication without a direct order from a physician.”

A pharmacist may switch between medications for a Medicaid beneficiary only if the replacement drug: (1) is therapeutically and pharmaceutically equivalent; and (2) costs less than the medication originally prescribed.

Of the \$35 million settlement proceeds, the federal government will receive \$18.6 million; the Medicaid programs in the 42 participating states and Puerto Rico will share \$16.4 million; and the whistleblower who alerted the government to Walgreens' misconduct will receive \$5 million. Walgreens also agreed to enter into a five-year corporate integrity agreement with the HHS Office of Inspector General as part of the settlement. (See *Health Care Compliance Reporter* ¶420,483). ■

U.S. Attorney, Northern District of Illinois Press Release, June 4, 2008.

In the News

SNF quality safeguards are insufficient, OIG says

Current mechanisms used to detect, monitor, and correct quality of care problems in skilled nursing facilities (SNFs) are insufficient because of procedural inefficiencies, communication breakdowns, and inconsistent citing of deficiencies and application of remedies, according to the HHS Office of Inspector General (OIG). In testimony before the House Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, OIG Chief Counsel, Lewis Morris, noted that program administrative oversight and enforcement systems are designed to identify poor care after its occurrence, instead of preventing the initial onset of problems. To address these issues, Morris said, CMS should: (1) improve screening of all SNF staff by creating a nationwide database accessible to the SNF industry; (2) create a demonstration project to establish mandatory compliance programs for selected SNFs; and (3) enhance the quality-of-care data made available to the SNF industry and the public.

OIG Testimony, May 15, 2008, Health Care Compliance Reporter ¶530,669.

EHR demonstration will improve quality of care

More than 30 communities have applied for a new demonstration project that will provide Medicare incentive payments to primary care physician practices that use certified electronic health records (EHRs) to improve the quality of patient care, according to HHS. The EHR demonstration project is expected to reduce medical errors and improve the quality of care for an estimated 3.6 million Americans, HHS said. Over a five-year period, financial incentives will be provided to as many as 1,200 small- to medium-sized physician practices in 12 communities, which will be selected in early June, for using certified EHRs to improve quality, as measured by their performance on specific clinical quality measures. Additional bonus payments will be available based on a standardized survey measuring the number of EHR functionalities incorporated by the physician practice. HHS predicted that total payments under the demonstration for all five years may be up to \$58,000 per physician or \$290,000 per practice.

HHS Press Release, May 19, 2008.

CMS announces bundled payment demonstration

CMS has announced a new demonstration for hospitals to test the use of a bundled payment for hospital and physician services for a select set of episodes of care to improve the quality of care delivered through Medicare fee-for-service. The goal of the acute care episode (ACE) demonstration is to use a global payment to better align the incentives for both types of providers and thus improve the quality and efficiency of the care delivered, CMS said. The demonstration also will test the effect that transparent price and quality information has on beneficiary choice and provider referrals for select inpatient care. CMS plans to competitively award only one ACE demonstration site per market area during the first year of the demonstration. The select sets of procedures included in the bundled payment demonstration include 28 cardiac and 9 orthopedic inpatient surgical services. The ACE demonstration is open to applicants from Texas, Oklahoma, New Mexico, and Colorado.

CMS Press Release, May 16, 2008.