

# MANAGED CARE

## OUTLOOK

The Insider's Business Briefing on Managed Healthcare

ASPEN PUBLISHERS

Volume 21, Number 23 • December 1, 2008

### At Presstime

#### Many Uninsured Children Have Insured Parents

Some 2.3 million children a year, mostly from low- to middle-income families, have no health care coverage to pay for preventive or other medical needs, even though at least one of their parents is insured, according to a new study supported by the Agency for Healthcare Research and Quality (AHRQ) and the National Center for Research Resources, part of the National Institutes of Health.

The new study is one of the first to examine the characteristics of uninsured children under age 19 whose parents were insured all year. These children account for a quarter of the estimated 9 million uninsured children in the United States.

Researchers studied 2002-2005 national data from AHRQ's Medical Expenditure Panel Survey and found that children from low-income families in which at least one parent had health insurance were more than twice as likely to be uninsured at some point during the year as were similar children from high-income families. They were also 73 percent more likely to be uninsured for more than six months.

For more information, go to [www.ahrq.gov](http://www.ahrq.gov). ■

 **Wolters Kluwer**  
Law & Business

### The State of the Hospitalist Industry Today and Tomorrow

*Adam Singer, MD*

With the number of hospitalists growing from zero to more than 20,000 in the 15-year history of the specialty, there can be little doubt that the vast majority of hospitals and managed care organizations (MCOs) remain both satisfied with and committed to the continued success of hospital medicine as the primary driver of inpatient care. The benefits of hospital medicine to all players in the system are now well documented in the medical literature. Recent studies confirm that hospital medicine groups (HMGs) yield cost savings of approximately 13 percent while delivering high-quality care and patient satisfaction.

*(See The State of the Hospitalist ... page 3)*

### Although a Relatively New Risk Area, Medical Identity Theft Should Not Be Taken Lightly

Imagine receiving a \$44,000 bill for a surgery you've never had or being told that your children are going to be taken away from you because your newborn baby tested positive for methamphetamines — and you don't even have a newborn baby. Frighteningly, these aren't "what if" stories but rather actual events that have occurred as a result of medical identity theft.

Medical identity theft is the inappropriate or unauthorized misrepresentation of individually identifiable health information for the purpose of obtaining access to property or services, which may result in long-lasting harm to an individual interacting with the health care continuum.<sup>1</sup> According to the Federal Trade Commission, medical identity theft accounts for 3 percent of identity theft crimes, or 249,000 of the estimated 8.3 million people who had their identities stolen in 2005.<sup>2</sup>

*(See Although a Relatively ... page 6)*

**EDITOR**

**Reba L. Kieke**  
Phone: 512/336-7262  
Email: rebakieke@austin.rr.com

**GROUP PUBLISHER**  
Paul Gibson

**EDITORIAL DIRECTOR,  
NEWSLETTERS**  
Ellen Ros

**Editorial Advisory Board**

**Garry Carneal**  
President  
InforMed  
Annapolis, Md.

**Norbert Goldfield, MD**  
Goldfield & Associates,  
Northampton, Mass.

**James M. Jacobson**  
Partner & Chair  
National Health Law Team  
Holland & Knight LLP  
Boston, Mass.

**Peter R. Kongstvedt, MD**  
Vice President  
Accenture  
Washington, D.C.

**Charles Stellar**  
Executive Vice President  
America's Health Insurance Plans  
Washington, D.C.

**Maureen E. Sullivan**  
Senior V.P., Strategic Services  
BlueCross BlueShield Assoc.  
Chicago, Ill.

© 2008 Aspen Publishers.  
All Rights Reserved.

**Managed Care Outlook** (ISSN: 0896-6567) is published twice-monthly by Aspen Publishers, 76 Ninth Avenue, New York, NY 10011. Send editorial correspondence to 2107 Old Mill Road, Cedar Park, Texas 78613. Send address changes to Managed Care Outlook, Aspen Publishers, 7201 McKinney Circle, Frederick, MD 21704.

To subscribe, call 800/638-8437. For customer service, call 800/234-1660. Annual Subscription Rate: \$632, plus postage, handling, and appropriate state sales tax. Single issues: \$24, plus postage, handling, and appropriate state sales tax. Multiple-copy rates available.

This material may not be used, published, broadcast, rewritten, copied, redistributed or used to create any derivative works without prior written permission from the publisher.

**Permission requests:** For information on how to obtain permission to reproduce content, please go to the Aspen Publishers website at [www.aspenpublishers.com/permissions](http://www.aspenpublishers.com/permissions).

**Purchasing reprints:** For customized article reprints, please contact *Wright's Reprints* at 1-877-652-5295 or go to the *Wright's Reprints* website at [www.wrightsreprints.com](http://www.wrightsreprints.com).

[www.aspenpublishers.com](http://www.aspenpublishers.com)

## National Briefs

**New Cases of Diagnosed Diabetes on the Rise:** The rate of new cases of diagnosed diabetes rose by more than 90 percent among adults over the last 10 years, according to a study by the Centers for Disease Control and Prevention (CDC). The data show that in the past decade, the incidence (new cases) of diagnosed diabetes has increased from 4.8 per 1,000 people during 1995-1997 to 9.1 per 1,000 in 2005-2007 in 33 states. The study used data from CDC's Behavioral Risk Factor Surveillance System and provides incidence rates of diabetes for 43 states and two U.S. territories. Only 33 states had data for both time periods, but 43 states collected data in 2005-2007. States with the highest age-adjusted incidence were predominately Southern states.

**URAC Rolls Out Revised Standards:** URAC has announced the rollout of significant revisions to its health information technology standards. The changes affect Health Web Site accreditation and URAC's Health Insurance Portability and Accountability Act (HIPAA) privacy and security standards. The revised standards clarify notice of privacy practices to consumers, including notice of material changes in privacy practices. Accredited organizations are now required to conduct a risk assessment. The risk assessment must include an analysis of the use of portable media such as USB drives and laptop computers — a need generated by an evolving technology landscape and highlighted by HIPAA security regulators.

**Study Says Online Health Coach Helps People Lose Weight:** OptumHealth Inc. recently announced the results from a 12-month study that found individuals who completed OptumHealth's Online Health Coach weight management program were 44 percent more likely to lose weight compared with those who did not complete the program. The study also found that individuals completing the program lost 63 percent more weight than those in a control group that did not go through the program. The Online Health Coach is available to employees and health plan members through private and secure Web portals, which serve as a foundation for building a culture of health and wellness within an organization by integrating content, wellness programs, phone-based disease and case management programs, tools, and trackers.

**NCQA and Pfizer Publish Strategies to Treat Tobacco Use:** The National Committee for Quality Assurance (NCQA), in collaboration with Pfizer Inc, has released a new publication, *Quality Profiles™: The Leadership Series — Focus on Tobacco Dependence and Smoking Cessation*, profiling evidence-based strategies for treating tobacco use and dependence. Effective tobacco management initiatives highlighted in *Quality Profiles* include efforts to encourage smoking cessation, prevent tobacco use, and reduce exposure to environmental tobacco smoke. ■

## The State of the Hospitalist ...

(from p. 1)

The Society of Hospital Medicine estimates that there are over 2,000 HMGs practicing in the United States today, with each group averaging nine to 10 hospitalists. A recently released annual survey conducted by the Society confirms that HMGs typically operate using one of two business models: doctors are either employed by hospitals or they are organized as private practice groups (private practice groups may be multispecialty or hospitalist-only). The two business models coexist in the market in roughly equal proportions.

### Seeking Optimal Alignment between HMGs, Hospitals, and MCOs

Hospital and MCO mandates to reduce costs, increase productivity, and continuously improve the quality of inpatient care challenges HMGs to be increasingly more proficient and productive in the delivery of their service. With an inherent advantage of independence and flexibility, it may be that the private practice model is better suited to meet these challenges going forward. Long-held concerns remain as to whether the hospital-employed model has the effect over time of blunting the HMG's focus on performance measures such as length of stay and readmit rates.

With increasing regularity, hospital executives are initiating strategic reviews of their HMG programs to determine if the business model in place continues to be the right fit for an individual facility. This is to be expected and welcomed as an opportunity to measure the HMG's alignment with hospital goals. Many hospitals are still working with the business model put in place when the decision was first made to bring an HMG into their facility. Predictably, these "first-generation" decisions, often made by long-gone executives, will be subject to periodic review. This is especially likely for HMGs that are not performing to expectations.

It seems to be a two-way street. Sometimes hospitals that have employed their own

physicians will conclude that bringing in a private practice group will give them better alignment with their own goals. Other hospitals conclude that a large investment in their own practice group will yield the alignment it seeks over the long term. Both strategies can work, and both strategies can fail.

The economics seem to favor the private practice model. The Society of Hospital Medicine reports in its recently released survey that hospital-employed hospitalists see nearly 25 percent fewer patients in a 12-hour period than their counterparts in larger private practice group organizations, with no reported differences in performance measures such as length of stay or readmission rates.

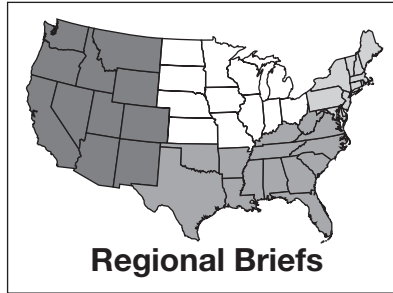
Yet even with a productivity advantage, many private practice groups face an uphill battle convincing hospitals and MCOs that they possess the business infrastructure to remain a stable and reliable partner over the long term. This is especially true for smaller single-site or highly regional groups, still present in large numbers in facilities across the country. Unwilling or unable to invest in the development of their administrative functions, small groups tend to fall back on their relationships and their history with MCO and hospital management as justification for their continued embedded status, but this justification increasingly falls on deaf ears in the C-suite.

Small practice groups that do not possess the capability to interface corporately with hospitals and MCOs increasingly are likely to be replaced or absorbed by larger private practice groups with a well-developed infrastructure including billing, recruiting, information systems, quality assurance, transition management, legal, and regulatory affairs. Indeed, some of the larger practice groups possess measurement and reporting capabilities along a broad array of metrics specific to the practice of hospital medicine that are considerably more advanced than what is otherwise available to the hospitals and MCOs they serve.

(See *The State of the Hospitalist ...* page 5)

## Northeast

**BCBSMA to Require e-Prescribing to Qualify for Incentive Programs:** Blue Cross Blue Shield of Massachusetts (BCBSMA) has announced that it will require physicians who prescribe medications to electronically prescribe in order to qualify for any of its physician incentive programs effective January 1, 2011. BCBSMA is introducing this initiative in an effort to continuously improve the quality, affordability, and efficiency of care for its members. The new requirement applies to both primary care physicians and specialists. Currently, 99 percent of primary care physicians in the HMO Blue Network and 78 percent of specialists participate in BCBSMA incentive plans. For additional information, go to [www.bluecrossma.com](http://www.bluecrossma.com).



beneficiaries at its facilities located inside the stores of retail giant Wal-Mart in the Greater Richmond, Va. market. The clinics are staffed by certified nurse practitioners who work with local physicians to diagnose, treat, and prescribe medications for common conditions such as

earaches, strep throat, and upper respiratory infections. RediClinic clinicians also administer a wide range of preventive services, including health screenings, vaccinations and flu shots, and physical exams. RediClinics are open seven days a week, and no appointments are necessary. For more information, visit [www.rediclinic.com](http://www.rediclinic.com).

**Humana and Metcare Announce Patient-Centered Medical Homes:** Humana and Metcare of Florida, Inc. announced the establishment of patient-centered medical homes for Humana Medicare Advantage members in nine Metcare centers in Central and South Florida. To accomplish this, the patient-centered medical home focuses on: ensuring that the patient has a personal physician that is coordinating all of his or her care with the team of health care providers; developing a patient-centered focus that delivers the right care at the right place, avoiding the need to visit the emergency room or retail medicine centers for nonemergency care; utilizing technology, such as electronic prescribing, to improve the quality and safety of care, and to increase member outreach to encourage preventive behaviors; and enhancing prompt access to care and increasing communication between physicians and members to better serve the patient's clinical needs.

## Midwest

**BCBSIL Sponsors "Marathon Kids" Program in Chicago Public Schools:** This year roughly 5,000 Chicago Public School (CPS) kids from 14 different elementary schools will participate for the first time in a running/walking program. Called Marathon Kids, the program is sponsored by Blue Cross and Blue Shield of Illinois (BSBSIL) and helps children complete a marathon over the course of the school year in increments of a fourth or half mile at a time. Participants typically will run or walk during their school gym classes and keep track of their progress using a mileage log. The log also helps them monitor what they eat and gives tips about having healthy amounts of fruits and vegetables daily. For more details, go to [www.bcbsil.com](http://www.bcbsil.com).

## West

## South

**Health Net Expands TRICARE Access through RediClinics in Virginia:** Health Net Federal Services, LLC, the government operations division of Health Net, Inc. has announced that RediClinic now welcomes TRICARE North

**Kaiser Adds New Health Tools to KP.org Member Site:** Kaiser Permanente has introduced three new online Healthy Lifestyle Programs on the topics of diabetes, depression, and insomnia. The new offerings are available to all Kaiser Permanente members at [www.kp.org](http://www.kp.org) and complement the site's current online health tools and programs on weight management, pain

management, smoking cessation, and more. The Healthy Lifestyle Programs are offered to members on kp.org through My Health Manager — a personal health record and one-stop resource for free, time-saving services, including emailing their doctor, refilling prescriptions, and checking lab results. Members also may schedule or cancel appointments online, as well as review recent office visits and recommended follow-up steps.

**Premera and Providence Reach Agreement on Rates:** Premera Blue Cross and Providence Health & Services have reached an agreement on rates that will keep Providence in Premera's provider network. As part of the agreement, Providence has withdrawn its termination notice. The agreement covers Providence's eight Washington hospitals and all of their employed and hospital-based physicians in the state. ■

## The State of the Hospitalist ...

(from p. 3)

### Are Hospital-Employed Hospitalists Worth the Risk?

Issues surrounding the management of the hospitalist workforce, perhaps, have the most consequence in deciding which business model best meets the needs of both hospitals and MCOs. The growing shortage of qualified hospitalists adds complexity to the equation. The hospitalist specialty is feeling the consequences of its own success; hospitalist medicine has more than 10,000 positions that are unfilled today. A hospital attempting to go it alone will quickly discover that its options for finding local inpatient physicians have dwindled to the point where it would be forced to recruit regionally and even at the national level in order to achieve and maintain its staffing quota.

Outsourced private practices carry the staffing burden themselves and should be capable of adjusting staffing levels more quickly and more cost-effectively than many hospitals can do for themselves. Additionally, outsourcing to an experienced private practice group ensures that regulatory hazards such as corporate practice of medicine and self-referral laws are effectively managed with minimized risk to the hospital and to the MCO.

Given the two distinct choices in employment models, hospitals that choose to directly control their HMG's physicians take the larger risk of misaligning the manifold objectives of quality inpatient care, high patient satisfaction, reliable staffing, improved utilization, and reduced cost. Moreover, from the perspective of the MCO

executive, the prospect of contracting with a hospital-employed group raises concerns that improvements to admit rates and resource utilization will be less of a priority due to possible conflicts of interest between what's best for the hospital and what is best for the MCO.

The private practice groups, especially the larger ones, have evolved to the point where they are capable of customizing their operations to accommodate the specific needs of each of the key stakeholders. With the right contracted group, an MCO likely can achieve better alignment on goals such as admit rates, readmission rates, specialist utilization rates, and the like.

### Future Challenges to the HMG Model

As the fast-growing specialty in the history of U.S. health care, hospital medicine has secured a leadership role in the delivery of inpatient care. Managed care executives should be receptive to opportunities for contracting with HMGs, particularly those in private practice, so that MCOs can benefit from the reduced costs and improved efficiencies that the hospital medicine specialty can provide. It is imperative, however, that managed care executives contract with HMGs that have the wherewithal to survive in the face of impending economic threats.

HMGs must learn to contend with business realities that many will find challenging and even life-threatening. The full import of the recent worldwide credit crisis, still making its way through the health care system, has yet to be fully understood or assessed. Many, though not all, HMGs are dependent on some type of

financial subsidy from their client facility in order to remain viable in their current form. HMGs, therefore, are vulnerable to cash flow or credit risks that hospitals will contend with in the future.

Private HMGs can expect to face increasing difficulty obtaining credit to run their business. In purely financial terms this means that many practices cannot truly afford to pay a new doctor while waiting for him or her to generate enough cash to pay for his or her salary and overhead. Should there be any change in reimbursement rates, or even the timing of payments from Medicare or insurance companies, many practices would not be in a position to fund base salaries.

Similarly, hospitalist groups that are employed by hospitals will begin to feel the pinch. Many of these programs are built on nonprofitable business models that for years

have been heavily subsidized by the hospital. One has to ask how long hospitals will be tolerant of this situation. It seems inevitable that the days of heavily subsidized hospitalist programs are going to have to come to an end, or the hospital inpatient program as we know it will not survive. I remain confident, based on my company's track record, that a debt-free and subsidy-free future is the best way to success for HMGs and their hospital and MCO clients. ■

Dr. Adam Singer is founder, chairman, and CEO of IPC The Hospitalist Company, Inc. a leading national hospitalist physician group practice company focused on the delivery of hospitalist medicine services. In October 2008, Dr. Singer was honored as Physician Entrepreneur of the Year by Modern Physician magazine. IPC's physicians and affiliated providers manage the care of hospitalized patients in coordination with primary care physicians and specialists. IPC provides its hospitalists with the comprehensive training, information technology, and management support systems necessary to improve the quality and reduce the cost of inpatient care in the facilities it serves. For more information go to [www.hospitalist.com](http://www.hospitalist.com).

## Although a Relatively ...

(from p. 1)

Understanding the scope and impact of medical identity theft can be daunting. It is a complex subject with many implications. Recently, the American Health Information Management Association (AHIMA) issued a practice brief<sup>3</sup> discussing medical identity theft, its ramifications, and how health care professionals and others can work together to prevent, investigate, and mitigate the damages it causes.

For starters, AHIMA separates medical identity theft into three categories. The first category includes those who obtain health insurance services through someone else's information. It is usually a friend, family member, or an acquaintance — basically, someone that has the opportunity to easily obtain someone's identity, impersonate that individual, and receive health care services fraudulently.

The second category involves an insider, usually an employee of a facility or even a doctor

that gets pulled into some type of organized crime ring or corrupt billing service. The Department of Justice estimates that someone's health insurance is worth between \$25 and \$50 on the street. As a result, crooks will go out and heavily pursue and buy and sell health information and often will get employees who work in facilities to steal patient information or get physicians or others in a position of authority to send in claims and create false billing accounts.

"These people are very quick about it," explains Harry B. Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA, director of Practice Leadership for AHIMA and co-writer of the practice brief. "Within 90 to 120 business days, they will come in and get your health information and file a bunch of false claims, and then, before the fraud can be detected by a payer's fraud and abuse department or the Department of Justice or the Office of Inspector General, the criminal is gone. Very often, people who have had their medical identities stolen will find out that somewhere else their information is being used yet again. Criminal elements actually sell the information among themselves."

The third and final category involves people who are involved in drug seeking behavior. They are either trying to get medication for their own use or to sell for a quick buck to support a drug habit. These individuals want to use another person's medical identity to secure prescription drugs.

### Gaps in the Privacy Rule

With all the privacy and security rules out there, it might be surprising to some that the problem with medical identity theft even exists. The trouble, says Rhodes, is that most of the problems have to do with the lack of a sound information security plan. While the Health Insurance Portability and Accountability Act (HIPAA) security rules may spell out what a facility needs to do to protect electronic health information and the privacy rules may explain what needs to be done to protect people's privacy, what often fails is the execution of those rules, says Rhodes.

A lot of facilities do identity proofing. This may seem like an effective measure, but it can actually cause significant problems if not carried out properly. For example, a patient comes in, and the receptionist asks to see a driver's license or an insurance card. Often, the receptionist will photo copy the two items and then put them in a drawer just on the other side of a reception counter. The problem is — anyone who wants to steal the photo copies can simply reach over and take a big handful out of the drawer and go out and sell them for \$25 or \$50 a piece.

There is an actual story in which a facility decided to start scanning the driver's license and insurance card of each patient that came in. The facility bought an elaborate system and scanned the information but did not put security controls on the software and hardware. This opened the door for a criminal to sneak in and steal the information directly from the files, and because they were digital images, the criminal was able to reproduce the driver's license as a perfect match.

Another problem often occurs when an employee resigns under pressure or resigns because of problems at work. An employee resigning is often treated differently from an

employee being fired. From the moment an employee is fired, he is often locked out of his desktop computer and is usually escorted from the building. The resigning employee, however, is often overlooked; there is often no urgency to terminate his computer access, and what about remote access? Because the employee is not being fired, everyone's guard is down. People forget to call information technology (IT) and remove the employee's access rights to the computer system, and now with so many remote employees the company forgets to remove remote access to the network. In many instances, what happens is that once the employee gets home, he can still dial in and retrieve data from his home computer.

In addition, organizations should divide job responsibility for critical tasks and introduce checks and balances. One person should not be able to do the entire billing process from beginning to end. Responsibility for the task needs to be divided between more than one person. That way, one person will not have the authority to create false claims and then turn around and create false accounts, et cetera. Divide the responsibility for the critical tasks up — one person could be in charge of submitting a claim, one might be in charge of receiving the claim, and another might be in charge of setting up an account. In addition, there should be oversight for the entire process.

Finally, there is the issue of access management. Does this scenario sound familiar? Someone gets promoted and changes jobs. Rather than updating the individual's access privileges to the appropriate level for the new position (which includes taking away old privileges that no longer apply), what happens is that IT just adds any new access privileges the person might have in the new job. The result is that the promoted employee now has increased access to computer functionality that he or she no longer needs in his or her new role.

Here is another scenario. The first day someone gets hired, IT calls and asks what access rights a new hire needs. The busy manager might say, oh, just give him the same rights as

so and so. Unfortunately, “so and so” may have a lot of system access rights that are beyond the scope of the new hire’s position, and now the new person will as well. The HIPAA regulations state that access to individually identifiable health information should be limited to the minimum necessary to perform the job.

### **The Cascading Effect of Medical Identity Theft**

AHIMA has created a diagram called “The Cascading Effect of Medical Identity Theft,” which demonstrates how medical identity theft affects an individual and his or her health care from the initial theft to corrupted health records. (See Figure 1) It begins with having health information stolen. A false claim is filed, a false record is created, and then the false information lives on. It is used for public health response, medical research, and payers that use the false information for pricing, staffing, contracts, and reimbursement calculations. It gets into the various databases and impacts decisions that are made based on the information in those databases.

### **What Can Be Done**

AHIMA stresses that there are a number of things that facilities can do to have a more secure health information system. First of all, organizations should do a risk assessment, says Rhodes. They should do it initially and ongoing. They should be looking for weaknesses, or risk areas, and solve them — immediately. And when they expand existing systems or buy new systems, they should go back and look at the problems they have had in the past and apply what they have learned to current and future systems.

According to AHIMA, a proper risk analysis includes the following elements:

- Asset inventory and prioritization;
- Threat and vulnerability identification;
- Examination of existing security controls associated with addressing identified threats and vulnerabilities;
- Determining the likelihood of exposure to identified threats and vulnerabilities;
- Determining the impact (fiscal, workflow, et cetera) associated with the exercise of a threat or vulnerability exploitation; and

- Determining, prioritizing, and mitigating identified risks.

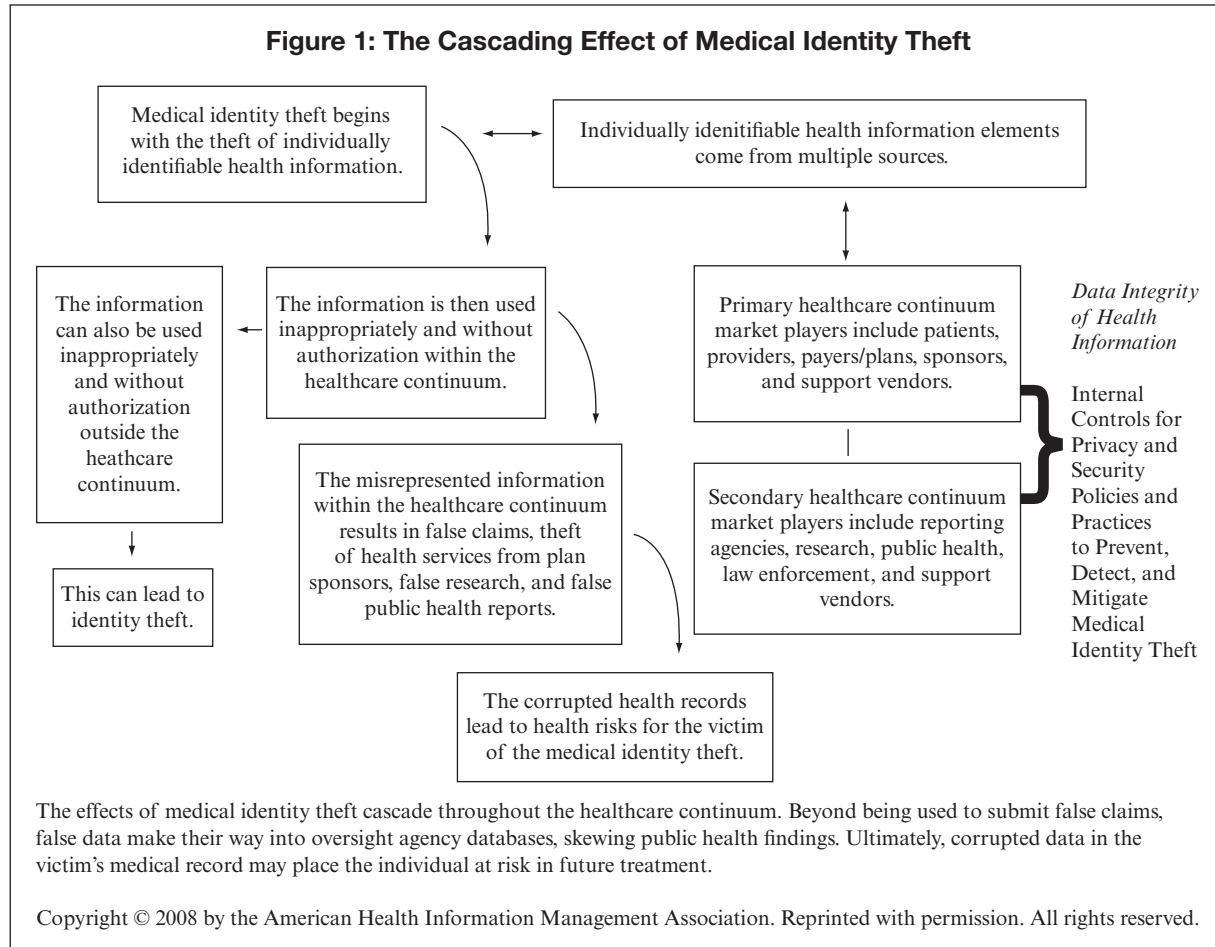
“Right now there are plenty of security standards and security technology out there if people would just apply them,” notes Rhodes. “When people buy systems, they need to do risk assessment early on. They need to start with a security administration plan. They need to evaluate how they are going to make the system secure. Some people think it’s too much trouble or too expensive, but the consequences of not having a secure system can be even more trouble and even more expensive.”

Take steps to empower consumers not to be victimized, says Rhodes. One way is through consumer education, either through a Web site or direct mail. Consumer education needs to let them know what they are supposed to do and also explain how important it is to keep their insurance card and insurance information just as secure as their credit cards and credit information.

Employ pattern recognition. When tracking health care data and submission data, be on the lookout for things that seem unusual (*e.g.*, an abnormally high number of hip replacements in one geographic area). Look for spikes in activity, and if a spike occurs, investigate the reason behind the spike. It could be warranted, but it could also be the result of fraudulent activity.

Plans can set up monitors, notes Rhodes. For example, some plans enlist the consumer; sending out an email to the patient as soon as a claim is filed. The patient has immediate knowledge that there has been activity on his or her account. If everything is okay, there is no problem. If something fraudulent has occurred, however, the consumer is empowered to notify the plan so action can be taken quickly to address the false claim. Not everyone has email, however, so controls need to be in place to reach even those who cannot be reached electronically, adds Rhodes.

Red Flag mechanisms are another way to track inappropriate activity. “When we were doing our research, we found that organizations were all over the board regarding who was responsible



for responding to medical identity theft; the designated staff member ranged from the risk management nurse to the compliance officer to the administrator to the director of health records to the director of nursing. You need to have an organized response,” explains Rhodes.

A growing number of facilities are creating what they call the data integrity specialist role. This role serves two purposes. First, the data integrity specialist helps ensure that the information in a patient’s record is accurate and timely and helps catch any errors that might occur on a day-to-day basis. In addition, the data integrity specialist also catches things like birthdays that do not match, diagnoses that do not match, and procedures that do not match. Many organizations do not even know they have a problem in this area until they hire a data integrity specialist, says Rhodes, and then they realize that the problem is bigger than they could have imagined.

Another purpose of the data integrity specialist is a little less obvious. Through the data integrity specialist role, if facilities are checking and investigating and reporting fraudulent activity, the activity can serve as a deterrent to those in the organization who might be tempted to commit a criminal act. If they know health data are being watched more carefully, they might just go somewhere else. Therefore, simply having this position and taking steps to track down criminal behavior can help minimize the risk.

Steps should be in place to quickly lock down a record and to create a John or Jane Doe record to extract data and pull out any information from a file that belongs to another person. This needs to be done to ensure that no information is left in a patient’s file that could result in a negative outcome in the future (e.g., data that could put a patient at risk of getting the wrong blood transfusion or the wrong medication).

There are a few other things that can be done, notes Rhodes. For instance, do background checks on new employees and even business associates — and not just when the relationship is first established but also periodically. Someone may have a squeaky clean background when first hired but could run into trouble a year or two down the road.

Make sure the facility has proper procedures for disposal of medical records. While it can be expensive to dispose of paper records and to “clean” a disk, it is essential to do so. Throwing files in a dumpster is not an option. Create a security administration plan to dispose of these files, and do not cut corners in this area.

#### Consumer Tips

The AHIMA work group also recommends the following seven preventive measures that consumers can follow to better protect themselves:

1. Share health and financial information only with trusted individuals, including providers.
2. Monitor benefits paid by health insurers.
3. Contact the insurer about charges for care not rendered.
4. Maintain copies of health records for comparison.
5. Check personal credit history for medical liens.
6. Safeguard all health insurance information including insurance cards, explanations of benefits, and correspondence.
7. Refuse to provide insurance information to solicitors.

“It is imperative for health care consumers to protect and monitor their health information with the same degree of diligence used to protect their financial information,” says Rhodes.

AHIMA has posted a checklist with additional guidance for consumers. For example, the first three tips are as follows:

1. Explore the resource “Tools for Victims” provided by the Federal Trade Commission (available online at [www.ftc.gov/bcp/edu/microsites/idtheft/tools.html](http://www.ftc.gov/bcp/edu/microsites/idtheft/tools.html)). Consider completing the universal affidavit to submit to creditors.
2. Review credit reports, correct them, and place a “Fraud Alert” on them.
3. If a Social Security number is suspected of being used inappropriately, contact the Social Security Administration’s fraud hotline at (800) 269-0721.

The complete checklist is available on the AHIMA Web site. ■

#### Endnotes:

1. The elements that define individually identifiable health information are listed in the HIPAA privacy rule, 42 U.S.C. Sec. 1320 d (6).
2. Federal Trade Commission. “FTC Releases Survey of Identity Theft in the U.S. Study Shows 8.3 Million Victims in 2005.” November 27, 2007. Press release. Available online at [www.ftc.gov/opa/2007/11/idtheft.shtm](http://www.ftc.gov/opa/2007/11/idtheft.shtm).
3. AHIMA e-HIM Work Group on Medical Identity Theft. “Mitigating Medical Identity Theft.” *Journal of AHIMA* 79, no.7 (July 2008): 63-69.

---

## CHCS Launches Initiative to Improve Quality in Practices Serving Diverse Populations

The Center for Health Care Strategies (CHCS) — a nonprofit policy resource center dedicated to improving health care quality for low-income children and adults, people with chronic illnesses and disabilities, frail elders, and racially and ethnically diverse populations — has launched the three-year *Reducing*

*Disparities at the Practice Site (RDPS)* initiative to support quality improvement in small physician practices serving racially and ethnically diverse Medicaid beneficiaries.

According to the Centers for Medicare & Medicaid Services (CMS), as many as 50 percent

of Medicaid beneficiaries under age 65 are racially and ethnically diverse<sup>1</sup> — a population that faces more barriers to care, greater risk of chronic disease, and higher mortality than whites. In addition, many Medicaid beneficiaries are served in small practices with only one to three providers. For example, a study that CHCS sponsored in Michigan, Arkansas, and Pennsylvania found that 50 percent of Medicaid beneficiaries were served in practices with three or fewer providers. In Michigan, 55 percent of African-American Medicaid beneficiaries receive care in practices with three or fewer providers.

Small practices often do not have the resources or infrastructure to dedicate to quality improvement projects. The *RDPS* initiative seeks to help leverage the support and resources that states and health plans can provide to these small practices and develop best practices for supporting quality improvement for low-resource provider practices.

The initiative is made possible by the Robert Wood Johnson Foundation and is being launched in four states — Michigan, North Carolina, Oklahoma, and Pennsylvania. These states were selected through a competitive, external review process. A request for proposals was released last year to states and to plans, and the RFP had to be submitted with a team (including state, plans, and provider champion) in place.

“We were looking for teams with a level of data sophistication to identify small practices, a demonstrated commitment for the project, and a clearly defined approach to improving quality and reducing disparities,” explains Lorie Martin, director of communications for CHCS. “We were also looking for a mix of delivery systems. Michigan and Pennsylvania are participating with health plan partners, and Oklahoma and North Carolina are implementing the project within their primary care case management programs. These states also all had significant existing practice improvement efforts.”

(See Figure 1 for a list of participating health plan partners in all four states.)

### Figure 1: Stakeholder Teams

**Michigan:** Michigan Department of Community Health, Great Lakes Health Plan, Health Plan of Michigan, Midwest Health Plan, Molina Healthcare of Michigan, OmniCare, Total Health Care, University of Michigan, Michigan State University, Greater Detroit Area Health Council

**North Carolina:** North Carolina Division of Medical Assistance, Community Care of North Carolina, Carolina Community Care Collaborative

**Oklahoma:** Oklahoma Health Care Authority, Iowa Foundation for Medical Care, APS Health Systems

**Pennsylvania:** Pennsylvania Office of Medical Assistance Programs, AmeriChoice, Health Partners, Keystone Mercy Health Plan, IPRO

Source: Center for Health Care Strategies.

The four state-led teams will seek to build the quality infrastructure and care management capacity of “high-opportunity” primary care practices where the greatest impact can be made. The following criteria will be used to identify these practices:

- Large volume of Medicaid patients;
- Racially and ethnically diverse patient panel;
- Large volume of patients with chronic conditions; and
- Opportunities to improve performance based on national quality indicators.

With technical support from CHCS and experts in the field, the teams will help practice sites implement interventions focused on:

- Identifying patients with chronic conditions and tracking outcomes using an electronic data management tool;
- Adopting evidence-based guidelines for targeted chronic conditions;

- Implementing culturally appropriate consumer self-management techniques; and
- Incorporating team-based care into ongoing practice operations.

In addition to the technical assistance, CHCS also will provide each team with \$200,000, to support project implementation.

CHCS and the initiative participants are currently in a planning stage for the initiative and are determining what supports the state teams will provide to the practices. Activities under consideration include providing practices with aggregated performance data; funding a nurse care manager and/or practice facilitator; supporting data registry approaches that are feasible for small practice sites; and providing technical assistance on how to efficiently implement evidence-based guidelines and tools.

The initiative will target improvements in diabetes care across designated small practices in the four participating states. An initial six-month planning stage will identify a mix of short- and long-term process and outcome measures, including standard HEDIS measures for diabetes care. Short-term results will include getting quality improvement activities implemented at the practice sites. CHCS expects to see improvements in infrastructure and process measures within the duration of the project, but it may take longer to see changes in clinical outcomes. Ultimately, “best practice” tools will be developed and shared with plans and states nationally to help influence additional quality improvement efforts at the point of care. ■

**Endnotes:**

1. Medicaid Statistical Information System State Summary FY2004, Centers for Medicare and Medicaid Services, June 2007.



Aspen Publishers  
Managed Care Outlook  
Distribution Center  
7201 McKinney Circle  
Frederick, MD 21704