Report on
MEDICARE COMPLIANCE

Volume 18, Number 15 • May 4, 2009

Weekly News and Analysis on New Enforcement Initiatives and Billing/Documentation Strategies

Contents

ZPIC Anti-Fraud Strategy Yields Fruit; New Warriors May Try Concordance Reviews

CMS zone program integrity contractors (ZPICs), the new Medicare fraud-and-abuse warriors, are already identifying potential fraud across the spectrum by cross-matching claims from Parts A through D, home health and durable medical equipment.

"We see migratory patterns of people who used to bill Part B and are now billing Part A," says Kim Brandt, director of CMS's program integrity group. These providers use the same Medicare provider number, but "they get caught in one thing, so they shift to another" (e.g., from durable medical equipment to home health). It was much harder to detect unscrupulous providers and suppliers when CMS relied on program safeguard contractors (PSCs), the precursors to ZPICs, because their work was doled out according to payment type. "Each PSC did its own thing" — Part A vs. Part B, etc. — "and no one contractor let us look across payment type," Brandt says. But ZPICs "only look at what's aberrant." Brandt spoke on CMS program-integrity initiatives April 27 at the Health Care Compliance Assn.'s Compliance Institute in Las Vegas and in an interview with *RMC*.

The role of ZPICs, she says, is to identify fraudulent behavior against Medicare and to ensure corrective action is taken. ZPICs also recommend administrative actions, such as suspensions, overpayment collections, referrals or sanctions. And they liaise with law enforcement, Brandt says. Finally, ZPICs use data analysis to "identify, monitor and track fraud, waste and abuse in Medicare." She notes that a lot of data analysis is

continued on p. 7

Second NY Medicaid Work Plan Warns That Compliance Failures Spell Personal Risk

New York State Medicaid Inspector General Jim Sheehan is putting board members of health care organizations on notice that if they drop the compliance ball, they will personally feel the heat.

"Where OMIG [i.e., the Office of Medicaid Inspector General] identifies a significant compliance or control weakness at a health care provider in the course of an audit, investigation or [data] match project, OMIG will inquire into the board's actions in assuring that compliance processes and systems are in place, and whether board members have exercised reasonable oversight over information and reporting systems," according to OMIG's Work Plan for state fiscal year 2009-2010, which was released April 27.

In appropriate circumstances, Sheehan tells *RMC*, "we will consider sanctions against board members when there are significant findings" (e.g., failure to fulfill their oversight and compliance responsibilities). Sanctions include censure and/or exclusion.

The details of board expectations will be fleshed out when OMIG publishes compliance-program guidance for hospitals and managed care organizations that do business

Published by Atlantic Information Services, Inc., Washington, DC • 800-521-4323 • www.AISHealth.com
An independent publication not affiliated with hospitals, government agencies, consultants or associations

with Medicaid. New York state requires all providers and suppliers to implement an effective compliance program if they collect $500,000 or more a year from Medicaid. This is OMIG's second annual Work Plan. The lengthy document summarizes the Medicaid audits and investigations planned by OMIG for the coming year. It's conceptually similar to the HHS Office of Inspector General's (OIG's) annual Work Plan.

Boston attorney Larry Vernaglia says boards rely on the venerated business judgment rule, which protects them from personal liability for their actions as long as they exercise their duties with due care and in good faith. Now it sounds like OMIG may be holding board members to a higher standard, Vernaglia, with Foley & Lardner LLP, tells *RMC*. OMIG's language — ensuring compliance processes and systems are in place and exercising oversight of information and reporting systems — sounds stricter than the business judgment rule, he says. With failure possibly meaning exclusion, Vernaglia adds, board members who work for other health care outfits doing business with Medicaid may quit so they don't jeopardize their careers. Their employers might force them to quit the board, he says. "There is risk that folks reading this might say, 'There is too much risk for my serving on this board.'" The board members might be thinking, "If problems happen that I should have found out about, I could be held liable," Vernaglia observes. "This could mean a loss of talent at companies when they are needed most."

OMIG Has Long List of Targets

Here is a taste of other OMIG Work Plan items:

◆ ***Ordering physicians:*** Medicaid spends a lot of money on diagnostic services and treatments ordered by physicians, some of whom aren't even enrolled as Medicaid providers. "We rely on their order as the basis for medical necessity of services," Sheehan says. Different kinds of abuses may pop up with ordering physicians. For example, a claim will be submitted with two names: the physician who performed the service and the physician who ordered it. Medicaid rejects the claim because the ordering physician has been excluded from Medicaid. Then the same claim for the exact same service is resubmitted with a different ordering physician's name even though the excluded physician is the true ordering physician.

◆ ***Medicaid has flagged certain DRG pairings*** that might involve upcoding from the lower to the higher-paying of the two. The Work Plan listed the DRGs that OMIG will focus on (some of which will be familiar from Medicare audits). *Among them:* (1) 014 (stroke with infarct) and 832 (transient ischemia); (2) 089 (simple pneumonias pleurisy — simple, complex older than 17 with clinical complications) and 541 (simple pneumonia and other respiratory disorders excluding bronchitis); and (3) 127 (heart failure and shock) and 544 (congestive heart failure and cardiac arrhythmia with major clinical complications).

◆ ***Credit balances***: OMIG has begun "credit balance audits of hospital medical accounts receivable with credit balances where Medicaid is the secondary payer. As part of our review, we will obtain from a hospital a listing of patient accounts receivable with credit balances where Medicaid is the secondary payer." The state is using a contractor to perform the audits.

The Work Plan's extensive audit and investigative items are a sign of how far Medicaid oversight has come in the past few years. State Medicaid program integrity and Medicaid fraud control units and CMS's Medicaid integrity program are intensifying scrutiny, and "people

Report on Medicare Compliance (ISSN: 1089-6872) is published 45 times a year by Atlantic Information Services, Inc., 1100 17th Street, NW, Suite 300, Washington, D.C. 20036, 202-775-9008, www.AISHealth.com.

Managing Editor, Nina Youngstrom; Associate Editor, Eve Collins; Editor, Michael Carbine; Executive Editor, Angela Maas; Publisher, Richard Biehl; Marketing Director, Donna Lawton; Fulfillment Manager, Gwen Arnold; Production Coordinator, Darren Jensen.

Call Nina Youngstrom at 800-521-4323 with story ideas for future issues.

Subscriptions to *RMC* include free e-mail delivery in addition to the print copy. To sign up, call AIS at 800-521-4323. E-mail recipients should whitelist **aisalert@aispub.com** to ensure delivery.

To order **Report on Medicare Compliance:**

(1) Call 1-800-521-4323 (major credit cards accepted), or

(2) Order online at www.AISHealth.com, or

(3) Staple your business card to this form and mail it to:
AIS, 1100 17th St., NW, Suite 300, Wash., DC 20036.

Introductory Discount Price:

Payment Enclosed* ❑ $468

Bill Me ❑ $498

*Make checks payable to Atlantic Information Services, Inc.
D.C. residents add 5.75% sales tax.

Subscribers to *RMC* are eligible to receive up to 12 Continuing Education Credits per year, which count toward certification by the Compliance Certification Board. For more information, contact CCB at 888-580-8373.

Call 800-521-4323 (or visit the Marketplace at www.AISHealth.com) to order ***Report on Medicare Compliance on CD***, a searchable CD with all issues of the newsletter published from January 2007 through December 2008. ($89 for subscribers; $389 for non-subscribers.)

may be blindsided by how aggressive their Medicaid [agencies] are," says Cheryl Rice, system corporate responsibility officer at Catholic Healthcare Partners in Ohio. States may be very aggressive if the budget woes have spurred cuts in Medicaid benefits, she says. For example, the hospital lab unbundling investigation, which originated in Ohio on the Medicaid side, was born "in crisis mode." Rice says compliance officers should adapt their programs accordingly.

Contact Vernaglia at lvernaglia@foley.com. View the Work Plan on the OMIG Web site at www.omig.state.ny.us/data/. ✧

Health System Tackles FTC Red Flags Rule With Risk Assessment

A risk assessment was at the heart of the development of the FTC Red Flags Rule identity theft prevention and mitigation program at Ohio State University (OSU) Medical Center. Identifying its risks — meaning the red flags unique to certain departments — and training employees in the hot spots were essential to the system's compliance with this new regulatory demand, officials there tell *RMC*.

But getting started with the risk assessment proved more challenging than anticipated because OSU Medical Center is a large, complex organization, says Privacy Officer Jennifer Cironi, who headed the task force/workgroup that developed the organization's Red Flags Rule detection and mitigation program, which includes a toolkit (see p. 4). The breakthrough came when a member of the task force, Tremayne Smith, manager of information security, devised a matrix to put in visual terms the four "points of entry" for customers' personal demographic and health information (the vulnerability for identity/medical identity theft).

The four points of entry are: (1) registration/scheduling (e.g., patients receive a new medical-record number at registration after sharing demographic information and showing identification); (2) clinical/patient care; (3) billing; and (4) employees (OSU Medical Center employees have electronic badges that can be used like a credit card to buy cafeteria food and gift-shop items. The tab is deducted from future paychecks). These departments are the heart of Red Flags Rule compliance because they all have "covered accounts."

According to OSU Medical Center's Red Flags Rule policy, a covered account means "a continuing relationship with a person allowing the person to conduct multiple transactions or make multiple payments in conjunction with obtaining a product or service primarily for personal, family or household purposes. Accounts include an extension of credit. Accounts include information maintained to allow a patient to obtain medical services prior to payment. Accounts include the right to use a card or badge to purchase items. Accounts include any type of account where there is a foreseeable risk to the patient or customer of identity theft."

FTC enforcement of the Red Flags Rule begins Aug. 1 (it was just moved from May 1). OSU Medical Center's Red Flags Rule task force began work in October, when it became clear the rules would apply to health care organizations. Red flags are patterns, practices or specific activities that signal possible identity theft. Examples of red flags include altered/forged documents, inconsistent photos/identification and duplicate Social Security numbers or Medicaid cards *(RMC 4/2/09, p. 4)*.

Cironi says Leslie Winters from the system's legal services department was indispensable in helping the task force understand the application of the covered accounts concept to departments at the medical center and other complex legal issues surrounding identity theft. This underscores the importance of drawing on many different skills when responding to the FTC's mandate, Cironi and Smith say.

Centralized Reporting Is Necessary

The departments with covered accounts conducted a risk assessment to identify compliance gaps. "We figured out where we were and where we needed to be for compliance," Cironi says. For example, the task force decided it needed a centralized reporting process for suspected identity theft, so it developed this procedure: A supervisor conducts an initial investigation. It may turn out that a report of suspected identity theft was actually a mistyped Social Security number, for example. But if the report raises more serious concerns, then the supervisor calls on the new "Red Flags Response Team." The team is comprised of Cironi and three other representatives, one each from patient accounting, medical information management and patient registration.

"The response team tries to resolve as many issues as possible," Cironi says. It does a lot of background investigations, working off information supplied by the supervisor who submitted the report. Particularly complicated issues are reported back to the system's identity theft workgroup, which was formed in 2007 to address identity theft issues generally.

A consistent complaint presented to the task force is patient reports of stolen identities. Either the patients received a bill for services they say they never received, or they reviewed their charge history and recognized claims that don't reflect services they received, Cironi says. "This is a red flag to us — we assume they are telling the truth — though there is a potential for identity theft to be misused" (i.e., as a cover story for patients

trying to escape responsibility for their bills). Sometimes OSU Medical Center lacks enough information to distinguish credible identity theft reporters from malingerers and it wants to be certain the investigation is as thorough as possible. So, Cironi says, "we are trying to find a consistent process to get us out of the CSI business while we maintain our focus on patient safety."

One option: The Ohio Attorney General (AG) has an identity theft passport program, and OSU Medical Center is considering ways to use that program when faced with patients who say their identity was stolen. Ohio citizens whose identities have been stolen (according to supporting documentation) will receive an "identity theft verification passport" from the AG that verifies that

Identity Theft and Red Flags Rule Toolkit

Ohio State University Medical Center has developed a multi-part toolkit to address identity theft and the FTC Red Flags Rule that includes a policy and procedure and answers to frequently asked questions (see story, p. 3). Below are two excerpts: a risk assessment and three examples of medical identity theft. Contact Privacy Officer Jennifer Cironi at jennifer.cironi@osumc.edu and Information Security Manager Tremayne Smith at tremayne.smith@osumc.edu.

Risk Assessment

Prevent					
		Yes	***N/A***	***Guidelines***	***Notes***
1.	Is there a shredder container easily accessible by staff?	❒	❒	*Contact your building's environmental services manager for questions about shredder containers.*	
2.	Are shredder containers locked? Are shredder containers emptied regularly?	❒	❒	*Contact your building's environmental services manager for questions about shredder containers.*	
3.	Is patient information containing names, dates of birth, and Social Security numbers stored in a secured area?	❒	❒	*Where is paperwork containing names, dates of birth, and Social Security numbers stored during the day/night? Is your area locked/restricted access? Remind faculty/staff about locking or logging off before leaving a work station.*	
4.	Has the use of Social Security numbers been eliminated from forms or computer systems wherever possible?	❒	❒	*Does your department use forms/store data requiring Social Security numbers? Is it a necessary data element?*	
5.	Are all portable devices encrypted?	❒	❒	*Contact the OSU Medical Center HelpDesk either by visiting OneSource > Quick Access > eHelpDesk, or by phone at 3-3861.*	
Detect					
6.	Have faculty and staff completed the mandatory Computer Based Learning Module related to Identity Theft?	❒	❒	*Complete the CBL here: http://edr.medctr.ohiostate.edu/CBL.html*	
7.	Do you know what Identity Theft Red Flags are pertinent to your area?	❒	❒	*An Identity Theft Red Flag is a pattern, practice or specific activity that would trigger staff of the possible existence of Identity Theft. Identity Theft Red Flags are unique to the area where you work.*	
8.	Have you reviewed and utilized the managers' toolkit related to Identity Theft?	❒	❒	*Access the Managers Toolkit via OneSource or call the Privacy Office at 3-4477.*	
9.	Are you aware of past instances of identity theft in your area?	❒	❒	*Examples of your Department's past experiences with ID Theft can give you clues to help you prevent and detect ID Theft in the future.*	
10.	Have you reviewed the Identity Theft Red Flags pertinent to your area with you manager, faculty, or staff?	❒	❒	*Remind staff to be aware of the unique triggers in the area where you work that may indicate an Identity Theft Red Flag.*	
Report					
11.	Do faculty and staff know to whom they must report activity related to identity theft?	❒	❒	*Remind faculty and staff to report suspicious activity related to identity theft to their manager.*	
12.	Do the managers know to report activity suspicious of identity theft to the Privacy Officer?	❒	❒	*Managers can call the Privacy Officer at 3-4477 who will alert the Identity Theft Response Team to further investigate suspicious activity. Issues not resolved by the Identity Theft Response Team will be further discussed and investigated at the multi-disciplinary Identity Theft Work Group.*	
13.	Do faculty and staff know to consult legal services prior to engaging police for issues related to identity theft?	❒	❒	*Identity theft cases are usually extremely complex and decisions turn on an analysis of many facts. Contact the Legal Services attorney on call for an assessment of whether engaging the police is appropriate for suspicious activity related to identity theft.*	

their information has been stolen. Patients can show the document when necessary to protect themselves or prove they are the real McCoy. Perhaps OSU Medical Center will direct victims of identity theft to this program and require a copy of that document before giving people a pass on their bills.

Another option: Some hospitals require patients to file police reports before they will waive hospital bills based on identity theft, Cironi says.

As part of the risk assessment, managers of various departments — including medical information management, hospital registration, gift shops, the Ohio State University Physicians' network and clinics — also identified the red flags unique to them. These include patients lacking identification, patients giving a date of birth that doesn't match their date of birth in the system, medical treatment that's inconsistent with a physical exam or medical history reported by the patient, e-mail or letters bouncing back repeatedly from more then one address for that patient, patients using a different name (they may look different but a hospital employee recognizes them), the same social security number used with different names, and patients reporting their identity was stolen.

The risk assessment has other elements as well. Department managers describe how covered accounts are open, list the types of covered accounts and report previous experiences with identity theft. Then, using a sample "standard operating procedure" (SOP) developed by legal, department managers craft their own SOP. While there is an overall policy governing OSU Medical Center's Red Flags identity theft program, the SOP is department-specific. It explains how the Red Flags Rule apply to employees and alerts them to the kind of suspicious activity they may confront in their day-to-day activities.

Also, all employees are required to complete Red Flag Rules computer-based training. It's done individually and can be tracked through OSU Medical Center's

Identity Theft and Red Flags Rule Toolkit (continued)

Examples of Medical Identity Theft

Stealing an Identity for Medical Care
Angela has an unusual medical condition, with frequent and painful episodes that require medical intervention. Angela did not have health insurance, but her friend, Beth, did. Angela borrowed Beth's identity. Each time Angela came in for services, she provided registration with Beth's name, date of birth, and Social Security number. Medical Center staff did not ask for a government-issued photo ID. After dozens of encounters over three years, the Medical Center was contacted by Beth's insurance company with suspicions of medical identity theft. The Medical Center Patient Identity Theft workgroup conducted an investigation and concluded that medical identity theft had occurred. The investigation included an interview with Angela, who confirmed the suspicions of identity theft. The medical records of both Angela and Beth were carefully reviewed and episodes of care were correctly reassigned to the right patient. Fortunately, Beth did not come in for services during the time period that Angela was using Beth's identity to receive care at the Medical Center. If Beth had sought services, then her care would have relied upon incorrect information in her medical record. The Patient Identity Theft work group took additional steps to correct the damage from Angela's medical identity theft, including correcting the billing of the episodes of care and coordination of future care for Angela.

Using Identities for Addiction
Bobby has an addictive disease and he is dependent on narcotics. He has refused offers for treatment for his disease. He visits emergency rooms and urgent care centers in the area with different conditions or injuries which include complaints of pain. Bobby no longer has insurance benefits, and he does not wish to attempt to re-enroll for any public assistance. Each time Bobby comes in to the Emergency Department, he provides a different name, usually a variation in the spelling of his name, a variation of his date of birth, and variations of his Social Security number. Since his data elements don't match, the registrar creates a new medical record number for each encounter Bobby has at the Medical Center. The Emergency Department clinical staff begin to recognize Bobby from earlier encounters and suspect he is using fake identifiers. The staff contact their supervisor, who directs the staff to follow an established procedure to attempt to obtain objective evidence of the patient's identity while the patient is still receiving services. In accordance with the Emergency Medical Treatment and Active Labor Act (EMTALA) and the mission of the Medical Center, the patient does receive services, but great care is taken to assure that the contents of his record are appropriately assigned to him. The case is referred to the Patient Identity Theft workgroup for review. Flags are placed in IDX and CAPI for other providers to be on alert for any subsequent registrations.

Patient Identity Mistakenly Used
Brian works in patient accounting. He receives dozens of calls daily from patients questioning and sometimes disputing their bills. One day, he received a call from a woman who reported that she had been contacted by a credit collection agency for an overdue payment to the Medical Center. Brian accessed the account and reviewed the dates of service with the caller. The caller continued to deny that she had received services on those dates and reported that she had not been in Ohio for more than 10 years. The caller was worried that someone had stolen her identity. Brian reported the situation to his manager and, together they turned the situation over to the Patient Identity Theft work group for further investigation. The work group was able to piece the history together and determine that the caller was not a victim of identity theft. Another individual with a similar name had been mis-registered using the caller's demographic information. The mis-registration was not uncovered during the episode of care and a bill was sent to the wrong person. The Medical Center contacted the collection agency, corrected the billing, and corrected the assignment of the medical record contents to the correct patient.

training system. Department managers can check the completion rate of their staff. Task force members will report completion rates to Cironi.

Training was developed with the help of the marketing department, which alerted the task force to various communication channels throughout OSU Medical Center, says Smith. "Without marketing, we wouldn't have known all the communication avenues" to pursue, Smith says. "Regardless of what you develop, you have to get it to people on the front lines and get feedback from them."

For example, marketing helped the task force develop answers to questions they anticipated employees would have about the Red Flags Rule. They are included in the toolkit. *Among them:* "What is the definition of medical identity theft?" "How can managers help educate their faculty and staff about what to do if they suspect identity theft is occurring or someone is trying to use a stolen identity?" "What are a patient's rights and responsibilities in regard to their identity?"

Also, the toolkit is posted on the OSU Medical Center intranet. And when employees sign on to their computers, they are met by a Web page with "buttons" on different topics they can "push" to link to more information. For one week, a button was identity theft. All this marketing will hopefully lead to publicity by word of mouth, Smith says.

Contact Cironi at Jennifer.cironi@osumc.edu and Smith at tremayne.smith@osumc.edu. ✧

IOM: Strengthened Conflict Policies, Some Regulations Are Needed

The Institute of Medicine (IOM) has released concrete advice for conflict-of-interest policies it says are necessary to protect against improper relationships between health care institutions and the pharmaceutical, medical device and biotechnology industries. While many hospitals have policies in place to address these relationships, the IOM report covers new ground that warrants attention from hospital compliance departments, one attorney who practices in this area tells *RMC*.

Most of the recommendations in the April 28 report are voluntary, but in some cases the IOM suggests that Congress and HHS should get involved. The IOM appointed a Committee on Conflict of Interest in Medical Research, Education, and Practice in 2007. The committee made the following recommendations:

◆ ***Academic medical centers, professional societies, patient advocacy groups and medical journals*** should establish conflict-of-interest policies requiring disclosure and management of individual and institutional financial ties to industries. These institutions should have committees to evaluate the ties.

◆ ***There should be standardized content, format and procedures*** for disclosing financial relationships to avoid variable policies and confusion.

◆ ***Congress should create a public Web site*** so companies can publicly report their payments to physicians, researchers, health care institutions, etc.

◆ ***Researchers should not participate in studies on human participants*** if they have a financial interest in the outcome of the project.

◆ ***Academic medical centers and teaching hospitals*** "should prohibit faculty from accepting gifts, making presentations that are controlled by industry, claiming authorship for ghost-written publications, and entering into consulting arrangements that are not governed by written contracts for expert services to be paid for at fair-market value."

◆ ***Facilities should restrict visits by sales people*** and limit the use of pharmaceutical samples to patients.

◆ ***There should be a new system for funding accredited continuing medical education*** that is free from industry funding.

◆ ***Meals, gifts and other relationships between industry representatives and physicians should be eliminated***. Professional societies and health care facilities should also have policies eliminating such relationships.

◆ ***Professional societies that draft practice guidelines should not accept industry funding*** for development of the guides and should exclude individuals with conflicts of interest from the projects. The groups also should publicly share their conflict policies, funding sources and financial relationships panel members have with industries.

◆ ***HHS should "develop a research agenda*** to create a stronger evidence base for future conflict-of-interest policies."

"Many conflict-of-interest policies predate the uptick in the level of scrutiny and attention [conflicts have received] in the past few years," says Washington, D.C., attorney Jennifer Geetter with McDermott Will & Emery. In addition, the report addresses institutional interests as well as imputed interests (interests held by key decisions makers that are imputed to the institution), which have not been addressed in many institutional policies, she explains.

"In addition, the policies that have existed in the past have, in certain cases, been principally informed by the federal regulation that exists with respect to FDA disclosures, NIH grant rules and general principles

of informed consent, but, even taken together, these regulatory responses do not answer all of the necessary questions in designing a comprehensive approach to reporting, assessing, managing, and overseeing conflicts of interest, she says.

The IOM is also broadening the scope of the policies by including continuing medical education and clinical care guidelines in its report.

Geetter says the process of investigating conflicts used to be discreet and straightforward for hospital compliance departments. "One of the challenges in management [of conflicts of interest] right now is most people recognize that they need to do it, but there are a lot of question marks around the how," she says. "Now institutions are looking for matches between individual interests, imputed interests and institutional interests," so the reporting, assessment, management and oversight processes have expanded and become more complicated, often cross-referencing activities that would otherwise not relate to one another. This has technological as well as culture challenges, she explains, as institutions need to address conflicts of interest system-wide.

"This is not just a compliance issue — it is a process issue. You can't effectively respond to a challenge unless you have a process in place that is flexible and elegant enough, that can handle all your problems, but is simple and transparent. And it has to be integrated into the other parts of your organization, and that's not always easy," she tells *RMC*.

Contact Geetter at jgeetter@mwe.com. Read the report at www.iom.edu. ✧

ZPICs Start to ID Possible Fraud

continued from p. 1

under way at law enforcement's request. The data are used in cases going to trial or settlement negotiations.

Because they can work across parts of the program, ZPICs might do concordance reviews, Brandt says. Concordance reviews involve auditors looking at both the hospital and physician claims for the same patient on the same date of service to determine if there is consistency in billing. Did the physician exaggerate the services performed based on the hospital's claim? Or did the hospital inappropriately bill for inpatient charges when the physician reported evaluation and management service reflecting observation services? Concordance reviews worry some providers, who haven't had a great experience with them in with other payers.

Brandt says "trigger points" for ZPIC reviews are aberrant patterns, such as (1) high utilization of services or items, (2) high-cost services or items, and (3) inadequate documentation submitted with a claim. All claims are potentially subject to review, but ZPICs have methods to target the suspicious ones. The volume reviewed "depends on the number of potentially fraudulent claims submitted by a provider," she notes. All the ZPIC data analysis under way is another reminder that providers should ramp up their data mining.

Seven ZPICs will audit the entire country, which is divided into seven zones based on Medicare administrative contractor jurisdictions. Zones four and seven are busy at work; "they became fully operational — which means the zones [were] handled by a ZPIC rather than a PSC — on Feb. 1, 2009," Brandt says. These zones include the fraud hot spots of Texas, New York, Florida, Illinois and California. The areas align with CMS program integrity field offices. Procurement for zones one and two is ongoing. No procurement is under way yet for zones three, five and six, she says.

Gabriel Imperato, an attorney with Broad and Cassel in Fort Lauderdale, Fla., says "there's every indication ZPICs will be more aggressive and penetrating than PSCs and other program integrity contractors."

Contact Brandt at Kimberly.brandt@cms.hhs.gov. ✧

NEWS BRIEFS

◆ **Michigan is now eligible to receive an extra 10% of recoveries from lawsuits brought under its state false claims law,** OIG told the state in an April 15 letter recently posted to OIG's Web site. Under the Deficit Reduction Act, states can qualify for the bonus if their statutes are similar enough to the federal False Claims Act (FCA). OIG invited states to submit requests for reviews of their laws to see if they are eligible. In late 2006, OIG told 10 states that their laws were not eligible for the reward, one of which was Michigan *(RMC 1/8/07, p. 6)*. Thirteen states have been deemed worthy of the incentive either because their laws were adequate or because they have amended their statutes to match the FCA, OIG says. Previously, Michigan's law required that a whistleblower pay the defendant's attorney fees and a $10,000 fine if the state declines to intervene in the case and the lawsuit is deemed frivolous. OIG felt this provision rendered the state's law less effective than the FCA, but the state has since amended the statute. Read the letter at www.oig.hhs.gov/fraud/falseclaimsact.asp.

◆ **One proposed fraud-fighting bill has been passed by the Senate, and another cleared a hurdle in the House,** congressional records show. The Fraud Enforcement and Recovery Act of 2009 (S. 386), sponsored by Sen. Patrick Leahy (D-Vt.), passed in the Senate April 28 by a 92 to 4 vote. The legislation includes provisions to strengthen the FCA, among other things. The Senate rejected an amendment that would have capped awards to whistleblowers, records show. Also, The False Claims Corrections Act of 2009 (H.R. 1788) was voted out of the House Judiciary Committee April 28 by a vote of 20 to 6. The legislation, sponsored by Rep. Howard Berman (D-Calif.), would close loopholes in the FCA by clarifying that the law covers fraud in federal programs even when the government uses contractors to administer the programs, and that an amended whistleblower complaint relates back to the original whistleblower complaint, among other things. Visit http://thomas.loc.gov.

◆ **General hospitals have not been adversely affected by specialty hospitals, says a study of three markets by the Center for Studying Health System Change (HSC).** The center monitored Indianapolis, Phoenix and Little Rock, Ark., to see whether the facilities, which normally specialize in cardiac and orthopedic care, are cherry-picking healthier and wealthier patients, as critics have alleged. General and safety-net hospitals have said they need these patients in order to subsidize services like the emergency room and care to indigent patients. General hospitals in the HSC study said they have had to aggressively compete for specialty doctors and have had challenges maintaining service volume and referrals. But while general and safety-net facilities reported that they are treating more indigent patients, many attributed this to the rise in numbers of uninsured patients, not to the specialty hospitals. Read the study at www.hschange.com.

◆ **All 15 nursing home corporations that entered into quality-of-care corporate integrity agreements (CIAs) with OIG between June 2000 and December 2005 enhanced their quality structures and processes,** OIG reports in an Office of Evaluations and Inspections report (OIE-06-06-00570) posted April 22. Three of the corporations initially resisted their monitors' guidance, but acquiesced after further OIG intervention, the report says. All of the nursing home companies monitored quality through internal self-assessment tools and by tracking complaints. All of the companies faced challenges in implementing the CIAs, including ensuring consistency in their quality programs at all levels of their organization, among other things. In its future oversight of CIAs, OIG says it will explore (1) responding swiftly to noncompliant corporations, (2) specifying requirements for documentation from facilities' quality committees, and (3) sharing lessons learned by corporations under CIAs and quality monitors. The report did not include any recommendations. To read the report, visit AIS's Government Resources at the Compliance Channel at www.AISHealth.com; click on "OIG Office of Evaluations and Inspections."

◆ **CMS issued a proposed rule April 28 that would update payment rates and "clarify the framework for Medicare patient selection and care" in inpatient rehabilitation facilities in FY 2010.** The proposed rule would be effective for discharges occurring on or after Oct. 1, 2009, CMS says. Comments on the proposed rule are due by June 29. The final rule is expected to be issued by Aug. 1. Visit www.cms.hhs.gov/InpatientRehabFacPPS/02_Spotlight.asp.

◆ **The Federal Trade Commission has delayed enforcement of the FTC Red Flags Rule until Aug. 1,** the agency said April 30. The FTC first moved the enforcement date from Nov. 1, 2008 (when the rule took effect), to May 1, 2009, because many health care organizations were not ready to comply. Visit www.ftc.gov/redflagsrule.

If You Don't Already Subscribe to the Newsletter, Here Are Three Easy Ways to Sign Up:

1. Return to any Web page that linked you to this issue

2. Go to the MarketPlace at **www.AISHealth.com** and click on "newsletters."

3. Call Customer Service at 800-521-4323

If You Are a Subscriber And Want to Routinely Forward this PDF Edition of the Newsletter to Others in Your Organization:

Call Customer Service at **800-521-4323** to discuss AIS's very reasonable rates for your on-site distribution of each issue. (Please don't forward these PDF editions without prior authorization from AIS, since strict copyright restrictions apply.)