Report on
Medicare Compliance

Volume 25, Number 38 • October 24, 2016

Weekly News and Compliance Strategies on CMS/OIG Regulations, Enforcement Actions and Audits

Contents

Managing Editor
Nina Youngstrom
nyoungstrom@aishealth.com

Contributing Editor
Francie Fernald

Executive Editor
Jill Brown

Internal Reviews of 340B Program Prepare Hospitals for HRSA Audits, Drug Refunds

When Medicare observation patients are admitted as inpatients, the drugs they were prescribed while outpatients may not qualify for 340B discounts. It depends on whether hospital policy determines patient eligibility at the time of the drug's administration. If the policy states the hospital determines patient eligibility at discharge, then the patient no longer qualifies for 340B drugs. Complicating matters, the patient could return to outpatient status before or after discharge and again be eligible for 340B drugs.

The intersection of these two compliance risks — the two-midnight rule and 340B — may not be well understood, but the reach of 340B underscores how much vigilance is necessary to ensure compliance with the drug-discount program at a time of intense 340B audits and new regulations. The HHS Health Resources and Services Administration (HRSA) is ramping up audits of "covered entities" and is slated to release omnibus guidance cracking down on them late this year.

"Doing your own internal audits will prepare you for when HRSA walks in the door because HRSA plans on visiting every organization and potentially more than once," said Cindy Bartlett, vice president of corporate responsibility at Bon Secours, a health system in eastern Virginia, on Oct. 7 at the Fraud and Compliance Forum sponsored by the American Health Lawyers Association (AHLA). "HRSA is increasing their audits significantly. 340B locations must be in compliance and prepared to prove that to HRSA during their audits."

continued on p. 5

CCOs May Have to Take Steps to Protect Themselves If They're Not Being Heard

Compliance officers may find themselves having to watch their back at the same time they are watching their company's back, an uncomfortable position to be in.

"It's no longer enough to tell compliance officers what their jobs are. It's to tell compliance officers how to protect their jobs as well as the organization," former federal prosecutor Andrew Grosso said Oct. 17 at the Healthcare Best Compliance Practices Forum in Arlington, Va., sponsored by the Health Ethics Trust.

He said some companies support their compliance officer's recommendations and recognize they have to do things the right way. "Other companies don't like the idea of someone in their midst, telling them what they are doing is wrong," said Grosso, with Andrew Grosso & Associates in Washington, D.C. "As compliance becomes more important, compliance officers are getting into things they probably would have left alone. So I see more compliance officers being the ones in trouble as opposed to the ones" whose findings are appreciated by senior leaders.

Compliance officers are inherently in "an awkward situation. You're asked to protect two masters: your company and the federal government," Grosso said. "Your

company needs to make money and the government spends money but wants to get the best bang for its buck — and the compliance officer is in the middle."

He advised compliance officers to think of this challenge in three parts:

(1) Doing their job effectively while protecting themselves. That includes staying on top of their performance appraisals, Grosso said. How have you been rated? Are there comments in the personnel file you were unaware of? "Make sure they're accurate, complete and if you disagree, try to correct or challenge them. Write a memo and put it in the file," he says. But don't do this surreptitiously, Grosso advised. "Keep your supervisor apprised of what you are doing. No one likes to be surprised," he said.

Compliance officers should be meeting regularly with the board of directors and talking to them during breaks. "Having a good relationship with the board is paramount if you are a compliance officer," Grosso said. Let board members know of developments in the field — including False Claims Act cases and OIG Work Plan items — and when you take actions in any of these areas (e.g., internal audits, investigations).

Report on Medicare Compliance (ISSN: 1094-3307) 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; Contributing Editor, Francie Fernald; Executive Editor, Jill Brown; Publisher, Richard Biehl; Marketing Director, Donna Lawton; Fulfillment Manager, Tracey Filar Atwood; Production Editor, Carrie Epps.

Subscriptions to *RMC* include free electronic delivery in addition to the print copy, e-Alerts when timely news breaks, and extensive subscriber-only services at www.AISHealth.com that include a searchable database of *RMC* content and archives of past issues.

To order an annual subscription to **Report on Medicare Compliance** ($764 bill me; $664 prepaid), call 800-521-4323 (major credit cards accepted) or order online at www.AISHealth.com.

Subscribers to *RMC* can receive 12 Continuing Education Credits per year, toward certification by the Compliance Certification Board. Contact CCB at 888-580-8373.

He also recommends that compliance officers define their job rather than deferring to management. Decide whether the compliance job is more about identifying and correcting problems or "running them up the flagpole for other people to correct," Grosso said. If it's the latter, compliance officers may be in a tough spot if an error they identified has persisted for a long time. "The company may not want to decrease the cash flow. What are you going to do to change it? Go in and get support for your position. Hire a [subject matter] expert and a lawyer."

Don't Keep Documents for Self-Interest

(2) Taking steps when they are not being heard about "a serious compliance problem."

When compliance officers make no headway in fixing errors, they are at risk if they do nothing, Grosso said. "If the government investigates, the question will be, what did you do? The government thinks you are the first line of defense. If it's willful blindness, that's tacit agreement, which is a form of conspiracy," Grosso said.

He advised compliance officers to document all the steps they took to get a compliance problem resolved, including reporting it to their boss and the board of directors. Compliance officers shouldn't feel pressured to allow written documents to be shielded by attorney-client privilege. "I find that's a second cousin to obstruction," he said. The same thing goes with being told to talk only to legal counsel. "You must be able to talk to the CEO and board of directors independently," he said. The solution: Get your own lawyer to help you figure out what to disclose, when and why.

It's OK to amass incriminating documents to help the government prove fraud, but not to protect yourself, Grosso said. It's a "tricky" area of the law. "If you take home documents to fight with your boss, you probably will be found in violation of [company] policy and it's a basis to fire you," he cautioned.

When compliance officers are at odds with the CEO about how to deal with a potential violation, they may consider going directly to the board. It's risky because compliance officers may become the scapegoat. "You have to make a judgment call. How serious is this and what will the repercussions be?"

Compliance officers may consider tape-recording their supervisor to obtain proof that a supervisor is trying to talk the compliance officer out of reporting a violation up the chain. Tape-recording people without their permission is legal in some states (e.g., Virginia), but not in others (e.g., Maryland). If compliance officers are fired because they engaged in protected conduct, they can sue to get their job back and damages. But was the conduct protected? "Tape recording someone can be protected

conduct but first it must be lawful activity," Grosso said. If it's lawful and the purpose of the tape recording is to stop the violation, then it's protected, he said.

If compliance officers are going to blow the whistle on their employer, they should look for a new job, perhaps before they go to the government. "There is a blacklisting possibility. No one wants a compliance officer who may go running to the government," he says. "I know the law says you can keep your job, but you won't be able to keep your job."

Grosso tries to talk people out of filing false claims lawsuits. "I let them know they are in for a really rough time." If they want to proceed, they should be confident that they are right and can prove it.

(3) What to do if the worst happens and compliance officers are fired.

"Raise bloody hell and let everybody know you are the good guy or you will be pegged as the bad guy," Grosso said. Talk to the newspaper, file a lawsuit, tell everyone you know, he said. "You don't keep your mouth shut and endure the slings and arrow of outrageous fortune."

They may file claims for retaliation under the False Claims Act. They don't have to prove there was a violation — just that they believed in good faith there was a violation, he said. The U.S. Court of Appeals for the D.C. Circuit has ruled that the statute protects whistleblowers while they are putting the pieces together, he noted.

It Helps to Be 'Influencer'

Two compliance officers who have felt supported by leadership in their careers say there will still be moments of tension, and that communication and documentation are essential to getting the job done.

Danette Slevinski, chief compliance officer for University Hospital in Newark, N.J., has worked at organizations with responsive leaders. But there have been times when she faced resistance to reviews of contracts or new technology, for example. "It has created friction between my position and management's position about what we need to do and why," she says. "There's a desire to quickly onboard," which doesn't always leave time for weighing fair-market value, privacy, security and other risks. "We had a healthy dialogue. I never had someone override my recommendations."

When compliance officers face a potential conflict, Slevinski recommends documenting their concerns and who they looped in internally (e.g., legal, billing) and externally (e.g., a fair-market value consultant). Come up with recommendations for solving the problem and examples of organizations that faced consequences for bad decisions. Two examples: Tuomey Healthcare System, which paid $72.4 million after losing a Stark and false claims case at trial over sweetheart deals with physicians *(RMC 10/7/13, p. 1)*, and its then-CEO, Ralph J. Cox III, who personally will pay $1 million in a settlement with the Department of Justice *(RMC 10/3/16, p. 1)*.

"If you're still not getting traction, you have a difficult decision to make," Slevinski says. "We don't sell widgets. We have one thing — our reputation — and we can never compromise our judgment."

Larry Pliskin, vice president of compliance at MediGold, a Medicare Advantage plan owned by hospitals and physicians in Ohio, said it helps to have skills as an "influencer" when facing resistance. "This is the ability to articulate a vision and get people to understand it. You have to communicate why something is a rule and that it impacts the organization in a certain way." Then document the risks to the CEO and board by email and memos, and follow up, asking "did you get my email? We can discuss the risks further. If we're found to be noncompliant, this is what will happen." Consider enlisting the support of outside counsel if you're not being heard, Pliskin says. At some point, though, some compliance officers may have to call it quits.

Contact Grosso at Agrosso@att.net, Slevinski at slevindl@uhnj.org and Pliskin at Larry.Pliskin@mchs.com. ✧

As Social Media Use Rises, Expect To Do More HIPAA Breach Analysis

As the use of social media continues to climb, hospitals will increasingly have to evaluate whether the information posted by employees is a HIPAA breach. Putting selfies on Snapchat when protected health information (PHI) is visible in the background may be in breach territory, but not every social media post will require reporting to patients and the HHS Office for Civil Rights. At the same time, hospitals shouldn't jump the gun when they are criticized by employees on social media because the conversations may be protected by the National Labor Relations Act.

"Social media as it relates to health care providers can be a landmine," says attorney Rebecca Romine, with Polsinelli in St. Louis. "Things that happen behind a provider's wall are typically considered confidential and private, but we are all human and have the ability to make errors. Because the things that occur behind walls may be interesting to the public and may be viewed as sexy, there is a great issue with people seeing that and wanting to share their experiences and doing it in an inappropriate manner to boost their self-esteem on social media."

The urgency for effective social media policies is mounting because activity on social media sites is growing by leaps and bounds, says attorney Tom Kiser, with

Polsinelli in Chicago. There are now 1.7 billion Facebook users, 1 billion people on YouTube and 255 million people using LinkedIn, he says. "People spend over 700 billion minutes a month on Facebook," Kiser notes.

Social media is also getting people into trouble with their employers. A study by Proofpoint, an Internet security firm, of companies with more than 1,000 employees found that 8% had fired employees over their social media use, and 15% had disciplined them, Kiser says.

Posts on social media sites may violate HIPAA and result in a breach, Romine says. "Obviously if PHI is posted on any form of social media, it's a disclosure," she says. For example, while full-face photographs are considered PHI, X-rays and imaging printouts (e.g., MRIs, ultrasounds) generally aren't — "but that answer is always qualified with the idea that if the X-ray or imaging result shows something so abnormal that you would be able to identify the individual, it would be considered PHI."

CMS Transmittals and *Federal Register* Regulations
Oct. 14 – Oct. 20

Live links to the following documents are included on *RMC*'s subscriber-only Web page at www.AISHealth.com. Please click on "CMS Transmittals and Regulations" in the right column.

Transmittals

(R) indicates a replacement transmittal.

Pub. 100-02, Medicare Benefit Policy Manual

- Internet Only Manual Updates to Pub. 100-01, 100-02 and 100-04 to Correct Errors and Omissions (SNF) (R), Trans. 228BP, CR 9748 (Oct. 13; eff./impl. Oct. 18, 2016)

Pub. 100-04, Medicare Claims Processing Manual

- Ambulance Inflation Factor for CY 2017 and Productivity Adjustment, Trans. 3625CP, CR 9811 (Oct. 14; eff. Jan. 1; impl. Jan. 3, 2017)

Pub. 100-07, State Operations Manual

- Revisions to Appendix W – Survey Protocol, Regulations and Interpretive Guidelines for Critical Access Hospitals and Swing-Beds in CAHs, Trans. 163SOMA (Oct. 14; eff./impl. Oct. 14, 2016)
- Revisions to Appendix J, Part II – Interpretive Guidelines – Responsibilities of Intermediate Care Facilities for Individuals with Intellectual Disabilities, Trans. 162SOMA (Oct. 14; eff./impl. Oct. 14, 2016)

Federal Register Regulations

Final Rules

- Merit-Based Incentive Payment System and Alternative Payment Model Incentive under the Physician Fee Schedule, and Criteria for Physician-Focused Payment Models (posted Oct. 19; Fed. Reg. pub. date, Nov. 4, 2016; eff. Jan. 1, 2017)
- Correction: Medicare Program; Explanation of FY 2004 Outlier Fixed-Loss Threshold as Required by Court Rulings, 81 Fed. Reg. 70980 (Oct. 14, 2016)

Even if they are generally directed at an individual, disclosures on social media are public because it's "not a secure method of communication," she says. If there has been a breach, which means PHI was acquired, accessed, used or disclosed in a manner not permitted under the privacy rule, it has to be reported unless there's a "low probability that the PHI has been compromised."

Analyzing Post Against Four Factors

To determine whether there was a low probability PHI was compromised, covered entities consider four factors, according to the HIPAA/HITECH breach notification rule, and there will be endless variations with social media:

(1) The nature and extent of the PHI involved: Look at what was in the post, Romine says. "To the extent the post is highly sensitive information — information related to mental health, HIV or STD status — that is not a good factor," she says. But it may be "innocuous" if the person just posted that "I get to see my favorite patient today."

(2) The unauthorized person who used the PHI or to whom the disclosure was made: It may be a positive factor if a physician "overshared a little bit in terms of asking for informal opinions" from colleagues on a LinkedIn group, she says. "That's a different scenario than if employee Joe Smith posted on Facebook for 3,000 friends that he saw his ex-girlfriend's medical records, and she tested positive for an STD," Romine says.

(3) Whether the PHI was acquired or viewed: "If something was posted on social media, unless there's a way to track if someone viewed the post, assume it was acquired or viewed," she says.

(4) The extent to which the risk to PHI has been mitigated: "Determine whether the post is still out there or has been deleted and whether it can be recovered from archived files on the Internet," Romine says. "I have found when we counsel clients on social media breach events, if an individual makes a post and reports it in a quick and timely manner, and it appears and disappears relatively quickly, it is a factor that can be taken into consideration as to whether privacy and security have been compromised."

While employees have to keep their lips zipped about patients on social media, the same doesn't hold true when talking about their employers. The National Labor Relations Board (NLRB) "will look to protect employees' right to engage in protected, concerted activity," as described by Sec. 7 of the National Labor Relations Act, says Robert Entin, with Polsinelli in Chicago. Sec. 7 gives employees the right to discuss the terms and conditions of employment. "Conversations around the water cooler are what the NLRB looked at to protect concerted

activity, but this water cooler is not as easily identifiable as it was in the last century. Now it's the virtual water cooler," he notes.

The NLRB ruled in favor of employees in several social media cases, Entin says. For example, Triple Play Sports Bar and Grille fired two employees after one posted a complaint on Facebook about the employer's tax withholding mistakes, and the other employee "liked" the posting. The bar contended the post was defamatory, but the "NLRB said that it is protected concerned activity" because liking someone's post is just like standing around a water cooler, shaking your head in agreement, Entin explains.

"The NLRB also is going after employers for overly broad handbook provisions," he says. The absence of examples of offenses in the handbook "can be found to violate the act." For example, if the handbook instructs employees to be respectful without providing examples, "it can be construed by employees to prevent them from engaging in protected, concerted activities."

Contact Entin at rentin@polsinelli.com, Kiser at tkiser@polsinelli.com and Romine at rromine@polsinelli.com. ✧

Prepare for 340B Audits

continued from p. 1

The 340B program requires pharmaceutical manufacturers to provide discounts on outpatient drugs purchased by covered entities that serve the nation's most vulnerable patients, including critical access hospitals, sole community hospitals, disproportionate share hospitals, freestanding cancer hospitals, children's hospitals, rural referral centers, federally qualified health centers and hemophilia clinics *(RMC 3/17/14, p. 1)*. They are subject to audit by HRSA and the pharmaceutical manufacturers that discount drugs. If covered entities run afoul of any program requirements, they are expected to repay drug manufacturers for discounts they weren't entitled to.

There are a lot of things that can go sideways with 340B compliance. Covered entities are permitted to dispense 340B drugs only to "eligible patients," which means the covered entities have established a relationship with the patients and maintain their medical records, said attorney Barbara Williams, who also spoke at the AHLA conference. It's considered "diversion" — a program violation — when 340B drugs are given to ineligible patients. That means, for example, the "hallway prescription" obtained by a nurse from a physician during work without a formal outpatient visit at the 340B entity or one of its child sites doesn't qualify for the 340B discount in the hospital's pharmacy.

Location also matters; 340B drugs may be covered in provider-based space if listed on the cost report and on the HRSA database as a child site of the main 340B parent site. That doesn't extend, however, to the hospital's outpatient dialysis clinic if it's operated by an independent company, Bartlett said. The physicians ordering 340B drugs must be employed or have a contractual relationship with covered entities. And disproportionate share hospitals, cancer hospitals and children's hospitals will be kicked out of the 340B program if they also buy drugs from a group purchasing organization, said Williams, with Powers Pyles Sutter & Verville in Washington, D.C.

Program requirements will soon become stricter when HRSA finalizes its omnibus guidance — also known as mega guidance — which is expected in December. In the proposed guidance *(RMC 9/7/15, p. 1; 8/31/15, p. 1)*, HRSA narrowed the definition of "eligible patient," clarified the definition of "covered outpatient drugs," addressed program eligibility and termination, and provided guidance relative to duplicate discounts for Medicaid managed care patients.

"Next year will be a big year of change in 340B," Bartlett predicted.

Bon Secours, which has a 340B coordinator, does monthly reviews of its 340B compliance. "Then we do more specific reviews if we find an area that keeps popping up," Bartlett said.

They gather data off an "accumulator," a computer system that sits on top of the billing system. It splits off drugs delivered on an outpatient basis from inpatient drugs; Bartlett noted that drugs used for inpatients are not eligible for 340B. "It's called a virtual inventory for purchasing more drugs," which means it informs the health system of how many 340B drugs were purchased and when to replenish the supply.

The 340B coordinator pulls data from the accumulator, purchasing and billing databases to review for 340B compliance. For example, "if the drug is ordered while the patient is an outpatient but not delivered until he's an inpatient, the drug no longer qualifies for 340B if your

policy states you identify eligibility at the time of discharge instead of at the time of administration," she said.

Internal audits help organizations become more familiar with where their data is. That's essential for the day when HRSA darkens your door. "You will need documentation for everything," Bartlett said. In advance of an audit, HRSA requires hospitals to send specific documentation for a specific timeframe. That data includes:

- ***The names of 340B drugs;***
- ***The names of drug manufacturers for each drug;***
- ***When the drugs were administered;***
- ***Dosages;***
- ***Patient identifiers for those who received the drugs;*** and
- ***Names of physicians who ordered them to determine eligibility.***

"You walk through the life of that drug and how it was purchased and dispensed and how you identified it as 340B," Bartlett said. "Every one of the elements must be proven."

Bartlett added that HRSA may ask for proof of credentialing or a contract with a physician who ordered 340B drugs during the audit timeframe. "Be sure you know who to call or how to get this information in advance of your audit," she advised.

It's not that mistakes won't be tolerated, but a lot is on the line with 340B compliance because hospitals could lose millions of dollars in discounts if they are removed from the program. That could have happened to one academic medical center (AMC) when it purchased a drug from a GPO. Hospitals in the program are limited to 340B drugs and wholesale acquisition cost (WAC). But in the midst of a drug shortage, the AMC couldn't find a medication from its usual wholesaler and, for a patient's sake,

Excerpt From 340B Spreadsheet for Drug Repayments

To ensure compliance with the 340B drug-discount program, Cindy Bartlett, vice president of corporate responsibility for Bon Secours, a health system in eastern Virginia, suggests hospitals use spreadsheets to track information about 340B drugs and potential errors that could lead to repayments to pharmaceutical manufacturers. Contact her at cindy_bartlett@bshsi.org.

Rebates for Ineligible Patients				
NDC Description	**Refill Times**	**Qty**	**MFT.**	**Amount Due**
XXX1 1-20 TABLET 28 EACH x 6	9	252		$72.34
XXX2 800 MG TABLET 180 EACH x 1	10	2400		$7,838.52
XXX3 90 MG TABLET 30 EACH x 1	2	60		$1,592.86
XXX4 10-325 500 EACH x 1	2	120		$5.54
	2	56		NA
CARVEDILOL 25 MG TABLET 100 EACH x 1	5	300		$22.75
	1	30		NA
			Total Refunds	**$9,532**

City	**State**	**Zip**	**Country**

Description	**Qty**	**Fill/Refills**	**WAC Cost**	**340B Cost**	**Refund**
XXX1 1-20 TABLET 28 EACH	28	9	$ -	$ -	$ -

Date	**Date**	**Date**	**Date**	**Date**	**Date**	**Date**	**Date**
12/10/2013	1/6/2014	2/3/2014	3/3/2014	4/1/2014	4/28/2014	5/27/2014	6/23/2014
16.61	13.68	13.68	13.68	13.68	15.36	15.36	15.36
7.03	7.03	7.03	7.03	7.03	6.79	6.79	6.79

had to buy it from a GPO. HRSA was informed and there was no penalty, but the lesson here was to be upfront and document every risky move, Bartlett said. "If HRSA does an audit, they will want to see all the documentation if you have to validate that the rules were followed or corrected," she said.

When hospitals identify potential mistakes, they have to repay drug manufacturers. "It's up to each organization to repay the manufacturer if they purchased inappropriately for the wrong patient or in the wrong amount," she said.

To streamline the process, Bon Secours has developed a template letter and spreadsheet (see box, p. 6). The template was written by its law firm. "When you repay the manufacturer, you want to have a template letter you can use from your attorney so you can be consistent and not make alarming statements," Bartlett said. "One of the first questions the manufacturer may ask is, how did you identify this error and why did this error occur? They also want to know if this is an isolated case or something you continue to address over time, or if HRSA is involved."

You May Have to Choose Manufacturers

In the template, hospitals can offer drug manufacturers three options for repayment: credit and rebilling, cutting a check or a reverse accumulation. The latter method is reserved for pharmaceutical manufacturers that don't respond to the letter or communicate with you in a defined timeframe.

Bartlett suggested attaching a spreadsheet to the template. The first page should have the manufacturer's name, address and contact person, which sounds like a no-brainer but isn't necessarily. That information is supposed to be in the database run by HRSA's Office of Pharmacy Affairs, but may be outdated. "We try calling the manufacturers before we send letters out to ensure we have the correct information, but it doesn't mean they call you back. Some manufacturers are overseas and hard to get in touch with," Bartlett said. And even some U.S.-based manufacturers' contacts change frequently.

The spreadsheet should quantify and explain the reason for the proposed repayment. Bartlett said hospitals need to "identify the time period of noncompliance for the manufacturers" when the drugs were purchased and when they were used. List the National Drug Code (NDC) number; the 340B or WAC; the difference between the 340B price and the WAC; and the proposed payback to the manufacturer.

Covered entities may find it worthwhile to hire a 340B coordinator, depending on how much money they save from the program, Bartlett said.

Contact Bartlett at cindy_bartlett@bshsi.org and Williams at Barbara.Williams@ppsv.com. ✧

NEWS BRIEFS

◆ **Omnicare Inc., the largest nursing home pharmacy in the country, has agreed to pay $28.125 million to settle allegations that it took kickbacks from Abbott Laboratories, a pharmaceutical manufacturer, in return for promoting the prescription drug Depakote to nursing home patients,** the Department of Justice (DOJ) said Oct. 17. According to the settlement, Omnicare is an institutional pharmacy that furnishes medication and pharmacy services to long-term care facilities and chronic care facilities. DOJ alleges Omnicare sought "illegal remuneration" from Abbott "in the form of agreements that required Omnicare to engage in certain promotional programs, grants, and other financial support" in exchange for promoting or buying Depakote between Jan. 1, 2001, and Dec. 31, 2008. DOJ contends the arrangement violated the anti-kickback law, and, as a result, false claims were submitted to Medicare, Medicaid and TRICARE, the settlement alleges. The case began with two whistleblower complaints that were consolidated by DOJ, which filed its own complaint in intervention in December 2014. Omnicare did not admit liability in the settlement. Ohio-based Omnicare was bought by CVS Health Corp. in 2015, six years after the alleged misconduct ended, DOJ said. Visit http://tinyurl.com/gnrbph4.

◆ **In a case related to meaningful use of electronic health records (EHRs), St. Joseph Health (SJH), a nonprofit integrated Catholic health care delivery system sponsored by the St. Joseph Health Ministry, has agreed to pay $2.14 million to settle potential HIPAA privacy and security violations,** the HHS Office for Civil Rights (OCR) said Oct. 18. SJH, which includes 15 hospitals and other entities in California, Texas and New Mexico, reported to OCR in February 2012 that some files it created for the EHR incentive program containing electronic protected health information (ePHI) were publicly accessible on the Internet from Feb. 1, 2011, to Feb. 13, 2012, through Google and perhaps other search engines, OCR said. "The server SJH purchased to store

NEWS BRIEFS (continued)

the files included a file sharing application whose default settings allowed anyone with an internet connection to access them. Upon implementation of this server and the file sharing application, SJH did not examine or modify it. As a result, the public had unrestricted access to PDF files containing the ePHI of 31,800 individuals, including patient names, health statuses, diagnoses, and demographic information." SJH agreed to a corrective action plan as part of the settlement. Visit http://tinyurl.com/j3bz4pb.

◆ **In the October issue of its *Medicare Quarterly Provider Compliance Newsletter*, CMS described billing errors identified by the comprehensive error rate testing (CERT) contractor and recovery audit contractors (RACs).** They include CERT findings of insufficient documentation for venous transluminal balloon angioplasty procedures, endovenous ablation therapy of incompetent veins and blepharoplasty procedures, and a RAC finding of improper hospital payments for discharged patients that should have been transfers when patients received post-acute care. Visit http://tinyurl.com/jkmqrw9.

◆ **CMS is now reporting progress in the Medicare home health pre-claim review demonstration and released preliminary data from Illinois.** According to its website, the time that the Medicare review contractor took to complete the review dropped from an average of 12 minutes to an average of nine minutes. "More requests are getting positive decisions," CMS says, with 66% being provisionally or partially affirmed by the eighth week. So far, the top reason for claim denials: skilled nursing services and/or therapy that wasn't medically necessary or documented. CMS says if they're rebuffed, home health agencies are permitted to keep submitting documentation to try to get their claims paid. The demonstration has not yet moved forward in the four other states (Texas, Florida, Michigan and Massachusetts). Visit http://tinyurl.com/hzv9o8g.

◆ **In a new report, the HHS Office of Inspector General (OIG) said CMS overpaid millions of dollars for chiropractic services in 2013 because most of them didn't comply with Medicare requirements.** OIG audited 105 chiropractic services and found 94 were not medically necessary. "On the basis of our sample results, we estimated that $358.8 million…of the $438.1 million paid by Medicare for chiropractic services was unallowable," OIG said. Medicare pays for active/corrective treatment for subluxation of the spine, as indicated by the AT modifier. Medicare doesn't cover maintenance therapy. "These overpayments occurred because CMS's controls requiring chiropractors to include the AT modifier and initial treatment date on claims were not effective in preventing payments for medically unnecessary chiropractic services." Visit http://go.usa.gov/xkdeW.

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 provide regular access to the newsletter — and other subscriber-only resources at AISHealth.com — 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.)