Report on
Medicare Compliance

Volume 24, Number 29 • August 24, 2015

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

Contents

Mercy Health, Clinic Settle Stark Case; MD Who Got Payments Is Whistleblower

Sometimes the physician who accepted big bucks from a hospital may become a whistleblower and allege the payments violated fraud and abuse laws.

At least that's what happened in the case against Mercy Health Springfield Communities, which owns a hospital in Springfield, Mo., and its affiliate, Mercy Clinic Springfield Communities. They agreed to pay $5.5 million to resolve allegations they violated the False Claims Act by having improper financial relationships with referring physicians, the Justice Department and the U.S. Attorney's Office for the Western District of Missouri said Aug. 13.

According to the settlement, the government alleges that Mercy Health and Mercy Clinic had financial relationships with more than 200 employed physicians that ran afoul of the Stark law. Mercy Clinic allegedly paid bonuses that took into account the value of the physicians' patient referrals for certain ancillary services.

The case (No. 13-3019-CV) originated with a whistleblower, Jean Moore, M.D., a board-certified pediatrician who was employed by Mercy Clinic Springfield Communities, which operates facilities in southwest Missouri. Moore filed a complaint in January 2013 and amended it that summer, and the Department of Justice later intervened.

continued on p. 6

Recent Data Breaches Raise the Stakes for Oversight of Vendors and Their Software

The reliance on vendors and the vulnerability of software is making health care organizations more vulnerable to breaches. Vendors, software or both were at the heart of recent HIPAA settlements with St. Elizabeth's Medical Center in Massachusetts and Anchorage Community Mental Health Services and reportedly let hackers inside the Target and Home Depot information systems (at least partly). Now that breaches are the new normal, covered entities, including hospitals, should have airtight business associate agreements, train employees to report suspicious activity and consider cybersecurity insurance, lawyers say.

"You want to be assessing vendors as part of your security risk assessment," says Minneapolis attorney Katie Ilten, with Fredrikson & Byron. Shortcomings in security risk assessments, according to the HHS Office for Civil Rights' (OCR) HIPAA audits of 115 covered entities, and the growing number of vendor and software-related breaches, are converging to raise the profile of vendor risks. The stakes will only get higher as OCR prepares to audit 150 more covered entities for HIPAA compliance and, for the first time, some of their business associates, Ilten says. "It's important to make sure you have those relationships in place."

The lack of a business associates agreement (BAA) played a role in last month's OCR settlement with St. Elizabeth's Medical Center, which agreed to pay $218,400 and implement a 12-month corrective action plan. The hospital's breach stemmed from its

use of an Internet-based document-sharing application to store the protected health information (PHI) of at least 498 people. The hospital had not done a risk assessment of the vendor providing cloud services and had no BAA with the vendor, Ilten says. An employee reported the problem directly to OCR. There was also an incident involving a stolen flash drive with 569 patients' PHI. That meant about 1,000 medical records in total potentially were exposed. In the settlement, the hospital agreed to do self-assessments and reporting on security vulnerabilities, and it will conduct 15 interviews and five surprise site visits to evaluate how well employees are complying with the hospital's privacy, security and breach policies.

Cloud services are tempting because they save organizations money, but don't assume they are diligent about security. "You've got to ask," says attorney Ann Ladd, also with Fredrikson & Byron, "and back yourself up with insurance." At the average health care organization, employees use 92 cloud services, often without the IT department's awareness, Ilten says. "If you are counsel, figure out what cloud services employees are using in all areas of the organization, and get business associate agreements, and do due diligence," she says.

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** ($728 bill me; $628 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.

Vendors were not the issue in the Anchorage Community Mental Health Services breach, but software and security failures were. In December 2014, the provider settled a case with OCR, paying $150,000 over the unsecured e-PHI of 2,743 patients, Ilten says. OCR found that Anchorage Community Mental Health Services didn't update its software with available patches, which resulted in vulnerabilities in its firewall, and hadn't done all the risk assessment required by the HIPAA security rule.

Two of the biggest breaches outside health care involved both vendors and software-patch failures, Ladd says. "It's likely hackers found out about Target's internal system design and vendor relationships from public postings," she says. Then hackers targeted a heating and air conditioning vendor and did a phishing scam. "They sent fake emails to vendor employees, hoping one would bite," Ladd says. An employee clicked on the link in the phony email, sending in the malware. "It was a system that could have been patched, but the vendor did not, and the consequence is the malware was installed on the vendor system," she says. The malware watched the traffic until the employee entered the Target system to do heating maintenance. "What happened after that is unclear, and there were also errors in the Target firewall." In the Home Depot breach, a hacker installed malware on a vendor's computer by compromising an employee's identification and exploiting the fact that the vendor didn't install a software patch, says Ladd.

Common Breach Themes: Vendors, Patches

In the Target and Home Depot cases, "you see a common fact pattern: Vendors were the road into the company systems, and it was through employee behavior and failure to patch and avoid malware." She notes that "70% of hacker attacks exploit known vulnerabilities where there is a patch that hasn't been installed." Also, Verizon reports that two-thirds of cyberscams use phishing, she says. "About a quarter of people were still opening [suspicious] email, and 11% were still opening attachments," Ladd says. That's why employee training should include practical tips on recognizing email scams.

Vendors that create, maintain, transmit or store PHI on behalf of covered entities must sign BAAs, which should always be at the covered entity's fingertips so it isn't scrambling in the event of a breach, Ilten says.

HIPAA requires certain elements in BAAs, but Ilten says covered entities may want to add protections. For example:

◆ ***BAA requirement: No use or disclosure of PHI other than permitted or required by law.*** Consider adding language barring the use or disclosure of any personally identifiable information or other confidential information

other than what's necessary for the vendor to perform services.

◆ ***BAA requirement: Use appropriate safeguards and conform to the security rule.*** Consider providing "contractually defined security measures," Ilten says, and requiring vendors to use industry standard security measures "as they evolve." Covered entities may want to require outside audits and certification.

◆ ***BAA requirement: Report unauthorized uses and disclosure to the covered entity.*** Consider requiring reports within two days so covered entities can comply with state breach notification laws and enforce contract rights.

There are other things to discuss with vendors that manage PHI, Ladd says. As part of their due diligence, covered entities should inquire about the vendors' disaster recovery program and back-up process (see below for a vendor questionnaire).

Also evaluate vendors' physical security at locations with your PHI. What about their policies and procedures? Their training and breach response? What if the vendor was on the OCR "wall of shame" for breaches? If so, ask the vendor how it fixed the problem that led to the breach. What assurance can the vendor give that it won't happen again? Is it reasonable to keep using it?

When it comes to insurance, covered entities may lean on their malpractice carrier for cyber liability coverage, which may be added at no expense, Ilten says. "But the limits are often terribly inadequate, so my advice to any health care organization is to seek out the best coverage," she says.

Contact Ilten at kilten@fredlaw.com and Ladd at aladd@fredlaw.com. ✧

Information Risk Management Questionnaire for Vendors

It's important for covered entities to "get evidence" that their vendors are on top of security, says Minneapolis attorney Ann Ladd, with Fredrikson & Byron (see story, p. 1). This tool, which was developed by the law firm, may help evaluate vendors' breach vulnerability. Contact Ladd at aladd@fredlaw.com.

Instructions: To be used for IT Security assessment of firm vendors who will host or manage firm data		
Vendor:		
Vendor Contact:		
Address:		
Vendor Contact Email Address:		
Vendor Contact Phone Number:		
[Customer] Contact:		
Please describe the Project: What services will be provided?		
Technical Diligence (Questions 1-8 pertain to cloud based services)		
Topic	**Response:**	**Comments:**
Audited Compliance or Certifications		
a) Have you been audited against any of the following guidelines or are you currently certified against any of the following standards? NIST, HIPAA, PCI DSS, ISO 27001, ISO 27002, SSAE16 SOC1 or SOC2, ISAE3402, CSA Cloud Controls Matrix, or other equivalent standard?		
b) Are you able to share with us a current report of the audit results?		
1. Physical Security		
c) Where is (are) your data center(s) located?		
d) Describe the physical security, disaster recovery, back up/redundancy, and prevention features of your data center		
e) Who (including data center staff, other employees and vendors) has physical access to the host servers?		
2. Network Security		
a) Are industry-standard firewalls deployed? Where are they deployed? Is the software and firmware on the firewall at a supportable level? Is administrative access to firewalls and other perimeter devices allowed only through secure methods?		
b) Does your company use intrusion detection systems (IDSs)? How long are IDS logs kept?		
c) Does your company use an intrusion prevention system (IPS)?		

continued

Information Risk Management Questionnaire for Vendors (continued)

Topic	Response:	Comments:
d) Are formal incident-response procedures in place? Are they tested regularly?		
e) Does your company engage third-party security service providers to perform ongoing vulnerability assessments?		
3. Systems Security.		
a) Are ongoing vulnerability assessments performed against the systems?		
b) Are file permissions set on a need-to-access basis?		
c) How are operating systems kept up to date? How does your company keep abreast of software vulnerabilities? What is the procedure for installing software updates?		
d) Are audit logs implemented on all systems that store or process critical information? How often are these logs reviewed?		
e) What change management procedures are in place?		
4. Staff Security.		
a) What are the credentials of the systems administrative staff?		
b) Has the systems administration staff undergone complete background and criminal checks?		
c) How long are the access logs retained for? Who reviews the logs? How many characters must a password have? Are alphanumeric passwords required? How frequently must it be changed?		
d) What are the on call processes for security staff?		
5. Security Policy.		
a) Describe the user account and password policy.		
b) Are screen-blanking mechanisms deployed on all employee workstations? Do sessions automatically time out after an idle period?		
c) Are user accounts for contract personnel created with expiration dates? How are user accounts closed after termination?		
6. Security Breach Response.		
b) Describe your security breach response policies.		
b) Have you experienced any security breaches in the past ____ months?		
7. Anti-virus Strategy.		
a) Describe your anti-virus strategy including the products you use.		
b) Where is the anti-virus software installed?		
c) How often do you update virus signatures?		
8. Disaster Recovery/Back Up.		
a) Describe your disaster recovery/back up policy.		
b) How often is your disaster recovery plan updated?		
c) Has your disaster recovery plan been tested?		
9. Privacy/confidentiality of data.		
a) How does your company protect the privacy of any information that may be collected and maintained through the software?		
b) Are your data centers SSAE16 audited and/or is your operating environment ISO 27001/27002 compliant?		
c) How is data integrity ensured?		
d) What checks are carried out on people who might have access to the data?		
e) Discuss all security features.		
10. Support Overview.		
a) Please describe the levels of support (i.e. technical, customer, etc.) your company provides.		
b) What methods would we use to contact your company for support?		
c) How many staff positions are available to assist with support issues?		
11. Transition Services.		
a) What happens to our data if we decide to terminate the license/subscription with your company?		

QIOs Begin Reviews of Patient Status Oct. 1, RACs in January

Quality improvement organizations (QIOs) will begin reviews of inpatient admissions on Oct. 1, as the audit ball bounces from one set of auditors to another. CMS is taking patient-status reviews out of the hands of Medicare administrative contractors (MACs) and limiting the role of the recovery audit contractors (RACs) to scrutiny of hospitals that are repeat offenders.

CMS announced the shift to the QIOs in the outpatient prospective payment system (OPPS) regulation proposed on July 1 *(RMC 7/13/15, p. 1)*, but it's a done deal and doesn't require the final rule to take effect. In an Aug. 18 open-door forum, CMS officials reiterated that the QIOs take control of the reviews in a little more than a month and explained a few of the particulars.

"QIOs will assume responsibility for conducting initial patient-status reviews to determine the appropriateness of Part A payment for short stay inpatient hospital claims that were previously conducted by MACs," and they will be based on current Medicare policy, said Steven Rubio, CMS beneficiary family centered care program lead. "Beginning on Jan. 1, QIOs and RACs will conduct patient-status reviews in accordance with any policy changes finalized in the OPPS rules and effective in January 2016." CMS proposed a hybrid model in which it again allows Part A payment for certain short stays, although it wouldn't be routine, and the two-midnight rule stays intact for patients expected to remain in the hospital for at least that long if physicians support their expectation in the medical record.

RACs will not be in the patient-status review business until Jan. 1, which means they can't audit claims to determine whether inpatient or outpatient/observation is more appropriate. But even then, their role is circumscribed. If QIOs identify hospitals with "persistent noncompliance with the Part A policy," including a high denial rate, disregard for the two-midnight rule and repeated submission of noncompliant claims after educational intervention, the QIOs will refer the hospitals to the RACs for "additional review," Rubio said. CMS has not yet defined what will push providers over the edge into "persistent noncompliance" but eventually will get there. "These parameters are still under review, and we will communicate them in the future," he said.

When the QIOs get to work, they will be bound by limits on the number of medical records — additional documentation requests (ADRs) — they can request from providers for short-stay reviews, Rubio said. "The ADR limits for those providers deemed large will be 50 medical records per year. For smaller hospitals, that number will be about 20 per year," he said. QIOs will get monthly reports of claims that are eligible for review. Those will be claims that have been paid by Medicare in the previous 90 days, he said. QIOs are expected to complete their reviews within 30 days of receipt of the medical records. Claims won't be denied until QIOs conduct educational sessions with hospitals, in which "QIOs had an opportunity to discuss the rationale for the denial and whether the provider can submit additional information to prevent the denial from occurring," Rubio said. "We are trying to design a highly collaborative process."

With Oct. 1 so close, hospitals will again face more scrutiny of admissions than they have in recent months. "It's time to put away the complacency," says Ronald Hirsch, M.D., vice president of education and regulations at Accretive Physicians Advisory Services. "I think some hospitals have used this moratorium as a free period and haven't been as diligent as they should be in reviewing short stays and potential short stays." It's going to be hectic, with the resumption of short-stay reviews coinciding with ICD-10 starting Oct. 1, he says. "Physicians will be bombarded by documentation requests — queries to

try to get them to give more specific documentation," Hirsch says. "Now is the time to get them to clearly document why the patient will be in the hospital more than two midnights."

Contact Hirsch at rhirsch@accretivehealth.com. Read CMS's announcement of the audit changes at http://tinyurl.com/p9ha9qh. ✧

MACs, QICs Can't Change Reason For Denial When Appeal Is Underway

For the most part, there won't be any more messing with the rationale for claim denials in the middle of the appeal process. CMS has instructed Medicare administrative contractors (MACs) and qualified independent contractors (QICs) to stick to the reason that the claim was rejected when they are considering appeals of post-payment denials, according to an Aug. 17 *MLN Matters* article (SE1521). But they have free rein when it comes to claim denials based on inadequate documentation and prepayment reviews. The new policy applies only to appeals received on or after Aug. 1.

Even with the caveats, the new policy is a relief for hospitals that have watched MACs and QICs transform their appeals of DRG coding denials into medical-necessity denials at redetermination (the first level of appeal) or reconsideration (the second level).

Keep an Eye on MACs, QICs

"I was glad to see this," says Denise Wilson, assistant vice president of clinical services for Denial Research Group/AppealMasters in Lutherville, Md. She suggests providers keep a close eye on MACs and QICs to ensure they adhere to the policy and "call them on the carpet if they don't." The bait and switch of coding and medical necessity denials has been a burden on hospital audit and appeals departments, she says.

In publishing its directive, CMS is formalizing a promise made by a top official at a June 25 forum on appeals held by the Office of Medicare Hearings and Appeals *(RMC 6/29/15, p. 6)*.

The *MLN* article says that when claims are denied by RACs, MACs, zone program integrity contractors or the comprehensive error rate testing contractor, MACs and QICs must limit their review "to the reason(s) the claim or line item at issue was initially denied" — except in the case of prepayment reviews. It's unclear why they are exempt. And if the provider failed to produce requested documentation, "claims initially denied for insufficient documentation may be denied on appeal if additional documentation is submitted and does not support medical necessity."

Wilson worries about this loophole. "I can read into that," she says. "What if they were initially requesting documentation for a coding issue, and you didn't respond to the ADR [i.e., additional documentation request], or you responded but didn't have everything they needed to make the decision? Then they look to see if it supports medical necessity. That has me a little concerned."

If the MACs and QICs run afoul of the new policy, hospitals should use that as grounds for appeal, Wilson says. "It always takes a little while to get things operationalized," but this is a meaningful change, she says. It will lift a weight off hospitals, which have lost DRG coding appeals for unrelated reasons. For example, she has been appealing the downcoding of DRGs by Performant Recovery, a RAC, on behalf of a hospital. "When we appeal to level one, to Novitas, if it is a three-day stay or less, it feels like they are automatically denying for level of care," Wilson says. If the patient had a three-day stay or less and the claim was denied for DRG validation, it's returned as not requiring inpatient admission. "Once you go to an appeal, it opens it up to any issue, but this is playing dirty," Wilson says. And eight of the cases, which had dates of service in 2014 and 2015, never mentioned the two-midnight rule, which means the MAC is using outdated admission criteria, she says.

For claims filed before Aug. 1, when the new policy took effect, hospitals are still vulnerable to the coding/medical-necessity switcheroo. It means hospital coders continue to work the coding side of the appeal, while clinicians are brought in to present the medical-necessity aspect.

Contact Wilson at dwilson@intersecthealthcare.com. Read the *MLN Matters* article at http://tinyurl.com/noo57ge. ✧

Mercy Settles Stark Case

continued from p. 1

In the complaint, Moore said she had been employed by Mercy since 1999, although it was known as St. John's Health System at the time. That year, the clinic became a separate entity from the hospital. According to the complaint, specialists employed by the clinic were "taxed" so the money could be redistributed to primary care physicians, such as Moore. "The redistribution resulted in 'PCP value payments' to Clinic primary care physicians of approximately $23,000 annually," the complaint alleged. The specialists said the payments hurt their ability to recruit other specialists, so the clinic ended them.

Next, in 2010, the clinic began "specialty funding" for some employed physicians that was not based on their productivity, according to the complaint. The mon-

ey allegedly came from the hospital, where clinic physicians referred patients for procedures and admissions. The payment per pediatrician, for example, allegedly was $39,000 in 2011.

In May 2012, Moore attended a meeting where clinic administrators said "there is a potential problem with the Clinic's compensation plan," especially in the wake of the 2012 decision by the U.S. Court of Appeals for the Fourth Circuit in the false claims case against Tuomey Healthcare System. "Clinic administrators explained that the financial relationship, whereby approximately $40 million flows from Mercy Health to the Clinic, creates implications under the Stark Law for Mercy Health," Moore alleged. But two weeks later, the clinic told Moore that specialty funding for pediatricians would rise to $48,000 each in 2013, the compliant alleged.

She also contended in the complaint that the clinic puts physicians in different "Stark groups" according to the volume of ancillaries they order. "Clinic physicians who order lots of ancillary services are placed in a group with similar high-volume orderers. The money for ancillary services goes into one pot for each subgroup and is divided among like type orderers in terms of how much a Clinic physician is paid for ancillary services," the complaint alleged.

A bonus pool can be bad news, depending on how it's done, says attorney Bob Wade, who was not involved in the case. If a clinic meets the Stark group practice exception, physicians can share profits from designated health services (DHS), but there must be at least five physicians in a bonus pool, says Wade, with Krieg DeVault in Mishawaka, Ind. "This hospital allegedly created multiple pools and put physicians in a pool based on the amount of referrals they generated," he says. "The relator said the pool the doctors went into was based on the volume or value of referrals they generated. That's inappropriate under Stark." A different kind of bonus pool led to the Stark-based false claims case against Halifax Health *(RMC 3/10/14, p. 1; 9/26/11, p. 1)*.

Bonus pools are appealing to hospitals because they love to use multiple methods to compensate physicians, Wade says. But if any of them are based on the volume or value of a physician's referrals, hospitals could have a Stark problem. Outside of health care, "you should be able to pay high generators more based on placing them in a bonus pool," he notes. But health care is in a parallel universe, which means placement in a pool should be based on specialty (if it's a multispecialty practice), location (if it's a multilocation practice) or other factors, but not the volume or value of referrals, Wade says.

It's a stretch, however, to find a Stark violation in a hospital's support for a subsidiary clinic, Wade says. Hospitals across the country lend money to their subsidiaries to cover their debts, including physician compensation. When subsidiaries are physician entities, they often suffer losses from the fact that their ancillaries (e.g., X-ray machines) are moved to the hospital after it buys the practice. "It's not inappropriate to lend money to a physician subsidiary," he says. Even if part of the money

CMS Transmittals and *Federal Register* Regulations

Aug. 7 – Aug. 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. 100-04, Medicare Claims Processing Manual

- October Quarterly Update for 2015 Durable Medical Equipment, Prosthetics, Orthotics, and Supplies Fee Schedule, Trans. 3323CP, CR 9279 (Aug. 14; eff. Oct. 1; impl. Oct. 5, 2015)
- Clarification of the Policy for Competitively-Bid Wheelchair Accessories Furnished with Non-Competitively Bid Wheelchair Base Equipment, Trans. 3324CP, CR 9272 (Aug. 14; eff. Jan. 1; impl. Jan. 4, 2016)
- Implementation of the Hospice Payment Reforms, Trans. 3326CP, CR 9201 (Aug. 14; eff. Jan. 1; impl. Jan. 4, 2016)
- New Waived Tests, Trans. 3327CP, CR 9261 (Aug. 14; eff. Oct. 1; impl. Oct. 5, 2015)
- October 2015 Integrated Outpatient Code Editor Specifications Version 16.3, Trans. 3328CP, CR 9290 (Aug. 14; eff. Oct. 1; impl. Oct. 5, 2015)

Pub. 100-07, State Operations Manual

- Revisions to Appendix J, Part II — Interpretive Guidelines — Responsibilities of Intermediate Care Facilities for Individuals with Intellectual Disabilities, Trans. 144SOMA (Aug. 14; eff./impl. Aug. 14, 2015)

Federal Register Regulations

Final Rule

- Hospital Inpatient Prospective Payment Systems for Acute Care Hospitals and the Long-Term Care Hospital Prospective Payment System Policy Changes and Fiscal Year 2016 Rates; Revisions of Quality Reporting Requirements for Specific Providers, Including Changes Related to the Electronic Health Record Incentive Program; Extensions of the Medicare-Dependent, Small Rural Hospital Program and the Low-Volume Payment Adjustment for Hospital, 80 Fed. Reg. 49325 (Aug. 17; eff. Oct. 1, 2015)

Proposed Rule: Correction

- CY 2016 Home Health Prospective Payment System Rate Update; Home Health Value-Based Purchasing Model; and Home Health Quality Reporting Requirements, 80 Fed. Reg. 49973 (Aug. 18, 2015)

for the loan was generated by technical revenue from hospital ancillaries and the physician is receiving compensation, in part, through the loan proceeds, it is too tenuous to connect the dots to Stark by alleging that part of the loaned money was generated through technical services, he says.

Atlanta attorney Alan Rumph also is skeptical that Stark is implicated when a hospital gives money to a subsidiary. "It's not necessarily a problem as long as the doctors don't have ownership in the clinic," says Rumph, with Baker Donelson. And while it's not a good idea to set up bonus pools the way this clinic allegedly did, he says hospitals are allowed to pay physicians DHS profits earned by a group-practice subsidiary. "You wouldn't be able to do that if doctors were direct employees of the hospital," Rumph says. The critical requirements are that each physician's compensation not exceed fair-market value for the services performed and not directly take into account DHS referrals to the group practice subsidiary or directly or indirectly take into account referrals to the hospital.

It was eye-opening that the whistleblower apparently received the bonuses that she contends implicated the Stark law and therefore the False Claims Act, Wade says. One message for hospitals: Think twice about telling employees their compensation may be questionable under the law, Rumph says.

Atlanta attorney Marlan Wilbanks, who represents whistleblowers, says the government is "keenly aware of whether a whistleblower was a material participant in the fraud being alleged" (although he is not commenting on the Mercy case). The share of recoveries can be limited, according to Department of Justice guidelines, if the whistleblower is seen as acting inappropriately, says Wilbanks, who is with Wilbanks & Bridges and represented the Halifax whistleblower. "In some cases, the whistleblower can be barred altogether from participating if they are active in material fraud," he says. When debating whether to accept a client, he looks at whether the would-be whistleblower attempted to stop the fraud or at least alert responsible parties inside the organization. "We try to make sure there is credible evidence the client protested the conduct and was not the architect or active participant in the fraud for personal gain."

Moore will receive $825,000 from the settlement, DOJ says. Her attorney didn't respond to *RMC*'s calls.

Mercy did not admit liability in the settlement, and its attorney had no comment. In a statement, Mercy said the physicians did not know of the "accounting error," which Mercy said it self-disclosed to the government after conducting its own investigation into allegations leveled by the false claims lawsuit.

Contact Wade at rwade@kdlegal.com. Visit http://tinyurl.com/qfgwalp. ✧

NEWS BRIEFS

◆ **A recent Medicare transmittal (3315) published on Aug. 6 has new and revised place of service (POS) codes for hospital outpatient departments.** CMS requires providers to put POS codes on all Medicare claims to report where services are provided. POS 19, which is brand new, is for "off campus-outpatient hospital." POS 22 is revised from "outpatient hospital" to "on campus-outpatient hospital." The codes were rolled out in response to CMS's plan to gather information on provider-based services, which was announced in the 2015 final outpatient prospective payment system regulation. In 2016, hospitals will have to start using a new modifier when billing for services rendered in provider-based departments, and physicians will use one of the two new POS codes *(RMC 11/10/14, p. 1)*. The mandate is seen as a possible precursor to reductions in payments to provider-based departments, which are higher than payments to freestanding clinics for the same services. Visit http://tinyurl.com/nv39mur to view the transmittal.

◆ **President Obama on Aug. 6 signed the Notice of Observation Treatment and Implication for Care Eligibility Act (H.R. 876), also known as NOTICE.** It requires hospitals to inform patients of their status (inpatient or observation) before discharge or within 36 hours after, whichever comes sooner *(RMC 8/3/15, p. 1)*. NOTICE was passed by the Senate on July 27 after it was approved by the House of Representatives four months earlier. Visit http://tinyurl.com/nghk8dg.

◆ **In an advisory opinion (15-11) posted Aug. 12, the HHS Office of Inspector General (OIG) approved a program to provide an antineoplastic drug for certain cancers free to patients for a little while pending insurance approval.** Even though the program potentially could implicate the anti-kickback law, OIG said it's low risk. One reason: Overutilization is not much of a threat given the fact the freebie is offered only to on-label uses of a specific drug and doesn't apply if insurance coverage kicks in within five days. Visit http://go.usa.gov/3HYFA.

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.)