

# Medical Practice Compliance

News, tools and best practices  
to assess risk and protect physicians

# ALERT

November 28, 2011 | Vol. 23, Issue 23

## IN THIS ISSUE

**RAC prepayment reviews part of new CMS demonstrations** 1

**HIPAA 5010 enforcement delayed** 1

**Analyze deals thoroughly to prevent possible kickbacks** 2

**ACO final rule relaxes several requirements** 3

**OCR poised to start new HIPAA audits** 4

**Case 72: The case of the 'recycled' PHI** 7

**SIUs yield a lot of power** 8

**Quick Compliance Quiz** Insert

## RACs will begin pre-payment review in 2012

Two new demonstration projects by CMS might mean you'll wait longer for payment next year. Starting in January 2012, Recovery Audit Contractors (RACs) in certain states will begin demonstration projects for prepayment review. In addition, Medicare Administrative Contractors (MACs) will conduct a demonstration that will require prior authorization for certain medical equipment claims, CMS said in a statement (*see box, pg. 6 for a list of demonstration states*).

"This likely will lead to higher costs for physicians and less care to beneficiaries," says James Pyles, principal at Powers Pyles Sutter & Verville P.C. in Washington, D.C., of the new demonstration projects.

**TIP:** Know what it is the MACs and RACs want to see in your claims, Pyles says. "If they want to see certain documentation, find that out up front."

(*see RACs, pg. 5*)

## Enforcement of HIPAA 5010 transaction standards delayed until March 2012

You've got more time to set up and test your use of the new version 5010 HIPAA transaction standards. CMS' Office of E-Health Standards and Services (OESS) announced Nov. 17 that it was delaying enforcement of compliance with the standards until March 31, 2012. The compliance date for using the standards remains Jan. 1, 2012.

OESS made the decision for a "discretionary enforcement" based on industry feedback that it's just not ready to implement the new transaction standards. Several of the problems included delays in receiving software upgrades, a low rate of timely adoption and insufficient testing of the new standards.

However, OESS will still accept compliance-related complaints. You must be prepared to produce evidence of your compliance or a "good faith" effort to become compliant during the 90-day period.

OESS does not clarify what constitutes "good faith" efforts to become compliant, but in reading the announcement it's not

(*see delay, pg. 6*)

## Analysis, proof of intent vital to identifying kickback schemes

When you think an insurance company is pressuring your practice to take part in an illegal deal, don't hesitate to perform a thorough analysis of the arrangement and push back when you feel like you're being asked to break the law.

**Example:** A pair of lawsuits against lab giants Quest and LabCorp have alleged that multiple large payers have been pressuring doctors to send all lab work to the two lab companies or face termination or non-renewal of contracts. The lawsuits also allege the actions by LabCorp and Quest were a violation of the federal anti-kickback statute and other laws.

As a result of the litigation, U.S. Senate Finance Committee chairman Max Baucus (D-Mont.) and ranking member Charles Grassley (R-Iowa) have demanded Quest and LabCorp as well as insurance companies United Healthcare, Aetna and Cigna turn over records that may show alleged overpayments from Medicare and Medicaid, according to a Nov. 8 article in *The Fiscal Times*.

**TIP:** Reach out through your practice's attorney to the payer's counsel and ask for an analysis of why the payer's proposal is legal – but don't approach the payer in a threatening manner, says Bill Maruca, a health care partner with Fox Rothschild LLP in Pittsburgh.

You can also take these three simple steps to prevent any involvement of your practice in a possible kickback scheme, according to Patric Hooper, a founding partner of Hooper, Lundy & Bookman in Los Angeles:

**1. Analyze.** Conduct a thorough analysis of the situation to determine whether it constitutes a potential kickback, Hooper says. "If someone says 'I'll give you X amount of dollars for every patient you refer,'" that is a warning sign, he says.

**2. Advise.** Warn your physicians not to partake in the alleged kickback, he adds. "Stress that it's more than just some kind of prosecution or civil action" based on the alleged kickback, Hooper says. "It can cause life-destructive collateral damage including losing your license, practice and exclusion from Medicare and Medicaid."

**3. Notify.** Get permission from your physicians to contact the company and tell them your practice will not participate, Hooper says. "If they don't stop pressuring you, tell them you will have no choice but to consider checking with the proper investigating agency."

**Remember:** Saying "but the payer made me do it" is not a valid defense, for either anti-kickback or Stark violations, Maruca says. "Historically, the feds have gone

### Subscriber Services

**President:** Steve Greenberg  
1-301-287-2734  
[sgreenberg@decisionhealth.com](mailto:sgreenberg@decisionhealth.com)

**Vice President:** Corinne Denlinger  
1-301-287-2363  
[cdenlinger@decisionhealth.com](mailto:cdenlinger@decisionhealth.com)

**Product Manager:** Karen Long  
1-301-287-2331  
[klong@decisionhealth.com](mailto:klong@decisionhealth.com)

#### Compliance Listserv:

To join our free Internet forum on fraud and abuse issues, go to <http://listserv.ucg.com/cgi-bin/listserv/listserv.pl/fraud-1>, click on the "Join the Fraud & Abuse Discussion Group" link, and follow the instructions.

#### Reprints:

To request permission to make photocopy reprints of *Medical Practice Compliance Alert* articles, or to obtain information on our copyright waiver, multiple copy and site license programs, please call us at 1-866-265-0148, or email Gary Belski at: [gbelski@decisionhealth.com](mailto:gbelski@decisionhealth.com).

#### Editorial:

**Director of Content Management:**  
Scott Kraft, 1-301-287-2361  
[skraft@decisionhealth.com](mailto:skraft@decisionhealth.com)

**Editor:** Chris Huntemann  
1-301-287-2722  
[chuntemann@decisionhealth.com](mailto:chuntemann@decisionhealth.com)

**Editor:** Marla Durben Hirsch  
1-301-299-6155  
[mhirsch@decisionhealth.com](mailto:mhirsch@decisionhealth.com)

**Chief Compliance Officer:** Sean Weiss  
1-301-287-2208  
[sweiss@decisionhealth.com](mailto:sweiss@decisionhealth.com)

#### How You Can Redistribute *MPCA*:

It is illegal to photocopy or electronically forward any part of **Medical Practice Compliance Alert** in paper or electronic form to anyone without our permission. It violates our copyright. But we understand that part of your job is to help educate and train others on how to comply with complex Medicare and Medicaid rules. The ability to share *MPCA* with staff members could be a key component of that effort, saving you a huge amount of time and money. That's why we offer a special, customized license to redistribute each issue. For more information, contact Gary Belski at 1-866-265-0148 or [gbelski@decisionhealth.com](mailto:gbelski@decisionhealth.com). In the meantime, if you received **Medical Practice Compliance Alert** and you are not the named subscriber, it is a violation of federal copyright law. However, only the party that provides the copyrighted material is at risk, not you. To confidentially report suspected copyright violations, call our copyright attorney Steve McVeary at 1-301-287-2266 or email him at [smcveary@ucg.com](mailto:smcveary@ucg.com). Copyright violations will be prosecuted. And **Medical Practice Compliance Alert** shares 10% of the net proceeds of settlements or jury awards with individuals who provide essential evidence of illegal photocopying or electronic forwarding of our newsletter.

#### Subscriptions:

For direct questions about newsletter delivery and account status, please contact DecisionHealth® at 1-855-CALL-DH1, or email us at: [customer@decisionhealth.com](mailto:customer@decisionhealth.com)

#### **Medical Practice Compliance Alert** is published 24 times per year by:

**DecisionHealth®** (a UCG company)  
Two Washingtonian Center  
9737 Washingtonian Blvd., Suite 100  
Gaithersburg, MD 20878-7364

**ISSN:** 1047-1863  
**Price:** \$547 per year  
DecisionHealth®, LLC

after the larger player in these matters, but that seems to be changing and they have been targeting physicians and other small fish lately.”

**Note:** There are portions of Stark law that relate to the ability of a managed care contract to compel participating physicians to refer within a network with certain restrictions, Maruca says. However, the exception does not apply to the Anti-Kickback statute.

“The Stark exception might apply to a typical managed care agreement that requires participating physicians to utilize other participating providers for testing [or] specialty services ... with appropriate exceptions, and in fact the patients generally do not have the same coverage for out-of-network services,” Maruca says.

But since the exception doesn't apply to the Anti-Kickback statute, “if the government can prove the payer intentionally offered inducements to refer, both parties are in violation,” he says.

**Note:** The Anti-Kickback statute is an intent-based statute, Hooper says. “You cannot be inadvertently guilty of breaking the Anti-Kickback law. The government has to prove you violated the statute and that violation broke the law and that you knew it was unlawful.”

— *Chris Huntemann* ([chuntemann@decisionhealth.com](mailto:chuntemann@decisionhealth.com))

## Final ACO rule reduces legal burden

It will be easier for your practice to work jointly with other providers in an accountable care organization (ACO) through CMS' Shared Savings Program than originally anticipated, thanks to a less stringent final rule published in the Federal Register on Nov. 2.

The ACO initiative, part of the Affordable Care Act, enables participating providers to earn incentive payments by working together in caring for Medicare patients and sharing in any savings generated by increased efficiencies and improved patient care.

The final rule relaxes several of the legal requirements that would have been imposed on providers participating in an ACO, according to attorney Matthew Amodeo, with Drinker Biddle in Albany, New York. Since ACO arrangements could violate the federal anti-kickback, Stark self-referral and antitrust laws, CMS – along with the HHS Office of Inspector

General (OIG), the Federal Trade Commission and the Department of Justice – had proposed waivers to help pave the way for you to participate in an ACO and share the savings (*MPCA 4/18/11*).

## 4 legal breaks in the final rule

The final rule makes joining an ACO even more enticing from a legal standpoint. The legal breaks include:

**1. Pre-participation waiver:** The Stark and Anti-Kickback laws would not apply to payments made before participating in the ACO, such as start up costs. Under this new waiver, hospitals could now bear the bulk of costs, such as the cost of forming the ACO and clinical management, according to attorney Lawrence Conn, with Foley & Lardner, Los Angeles. “Currently [under Stark] hospitals could only subsidize 85% of an electronic medical record (EMR). Under this waiver, hospitals can subsidize the whole EMR,” Amodeo says.

**2. Participation:** The Stark and Anti-Kickback laws would not apply to CMS payments of shared savings

### ACO rule relaxes certain compliance obligations

Providers who take part in accountable care organizations (ACOs) will face a host of new legal burdens. However, in the final rule CMS softened some of these more “practical” burdens, according to Matthew Amodeo, with Drinker Biddle in Albany, New York. Here are four ways the final rule may make participation in an ACO easier from a compliance standpoint:

1. Less burdensome reporting requirements. The required number of measures has dropped from 65 measures to 33 measures.
2. No more electronic health record (EHR) mandate. The final rule eliminates the requirement that at least 50% of physicians in the ACO must meet the meaningful use requirements in the EHR incentive program, although EHRs will still be a quality measure.
3. Streamlined governance. ACOs no longer must provide proportionate representation on their boards.
4. Ownership allocation and savings amount restrictions eliminated. “So a hospital can provide 99% of the capital and doctors can take 99% in the shared savings,” says Amodeo.

received for activities “reasonably related” to the ACO’s operations. The proposed rule would apply the waiver only to activities “necessary for and directly related to” its operations.

**3. Waiver for patient incentives:** Providers may now provide certain in-kind services to patients for free or at reduced prices without worry of the Stark and Anti-Kickback laws. The anti-kickback and Stark waivers were presented in conjunction with the final rule as an interim final rule with the opportunity to comment until Jan. 3, 2012. **Note:** The waivers do not apply to financial incentives such as waiving a patient’s copayment.

**4. Antitrust:** Antitrust review of the ACO is no longer mandatory. So it will not only be easier to form and operate an ACO, providers won’t incur as much in legal costs to deal with the review, says Amodeo.

The final rule also changed some of the financial provisions of the program to make it more enticing to providers, such as a new risk-free track allowing providers to share only in savings, not losses; upfront payments to help with capital costs; and earlier kick-in of the shared savings. **Note:** See the story on pg. 3 for ways in which the final rule relaxes your compliance burdens.

## ACOs still not a bed of roses

While joining an ACO is now more attractive than before, there are still many hoops to go through. “Whether it’s good for a physician may depend on his or her specialty. If you have a high Medicare population, you may want to join one,” says Amodeo.

Moreover, there are some issues physicians in particular should keep an eye out for. For instance, the Anti-Kickback and Stark waivers are subject to change. The new waivers are “broad enough to drive a truck through,” says Amodeo. CMS and OIG have already indicated that they will narrow the waivers in 2013, he says. So an arrangement that passes muster now may run into compliance trouble in little less than two years.

Physicians also need to ensure that their documentation is in order, such as participation agreements, shared savings allocations and the like, since CMS doesn’t want the relaxed compliance rules for ACOs to spill over into non-ACO arrangements where they may not pass legal muster, warns Conn. “Make sure your i’s are dotted and your t’s are crossed,” he says. — *Marla Durben Hirsch* ([mhirsch@decisionhealth.com](mailto:mhirsch@decisionhealth.com))

### On the Internet:

- ▶ ACO final rule: [www.gpo.gov/fdsys/pkg/FR-2011-11-02/pdf/2011-27461.pdf](http://www.gpo.gov/fdsys/pkg/FR-2011-11-02/pdf/2011-27461.pdf)
- ▶ Interim final rule on waivers with instructions for submitting comments: [www.gpo.gov/fdsys/pkg/FR-2011-11-02/pdf/2011-27460.pdf](http://www.gpo.gov/fdsys/pkg/FR-2011-11-02/pdf/2011-27460.pdf)
- ▶ New antitrust guidance: [www.ftc.gov/os/fedreg/2011/10/111020aco.pdf](http://www.ftc.gov/os/fedreg/2011/10/111020aco.pdf)

## OCR to start auditing providers for HIPAA compliance

Expect to see a lot more focus on your compliance with HIPAA’s privacy and security rules. HHS’ Office of Civil Rights (OCR) has finally begun to audit covered entities – and you can be a target as early as this month.

OCR will initially audit 20 covered entities and will perform up to 150 audits overall through December 2012, according to its Nov. 8 announcement. OCR will use this pilot audit program to examine the mechanisms for compliance, identify best practices, and discover risks and vulnerabilities that haven’t otherwise come to light through the complaint process or security rule breach reporting.

The HITECH Act, which amended HIPAA in 2009, required HHS for the first time to conduct random audits to check for HIPAA compliance. OCR appeared to have some trouble getting this program off the ground at first (*MPCA 6/13/11*), but eventually engaged accounting firm KPMG to create protocols for assessing compliance and conduct the audits on OCR’s behalf (*MPCA 7/25/11*).

### Details still sketchy; compliance window small

OCR has been relatively open about how the audit process will work, says Jan McDavid, compliance officer and general counsel for consulting firm Healthport, in Alpharetta, Ga. OCR will notify you by mail if you are an audit target (a sample notification letter is on OCR’s website).

The audit will occur within 30 to 90 days, and will include a site visit, which could take three to ten business days and involve interviewing staff and observing procedures and operations. KPMG will issue a draft report, which you will have a chance to comment on, and a final report will be submitted to OCR.

The notification will be accompanied by a letter from KPMG, which will request “certain information” to “facilitate” the audit. The audit process is slated to take 90 days total, but since OCR so far hasn’t met any of its timeframes for this project, that timeline may be adjusted, says McDavid.

However, the process still leaves several unanswered questions:

- **What “certain information” will KPMG be requesting to review before the audit?** Since there’s no sample KPMG letter on OCR’s website, it’s difficult to ascertain, although it’s likely to consist of a practice’s policies and procedures and other documentation of its HIPAA compliance program, such as copies of the most recent risk assessment.

**What’s worse:** You have only **10 business days** to pony up this documentation to KPMG. You don’t want to be scrambling to create this documentation during those 10 days. “OCR will look to see when those policies and procedures were enacted, so you could be under even more scrutiny [if you’re unprepared],” warns attorney Michael Kline, with Fox Rothschild in Princeton, N.J.

- **What will KPMG be looking for?** OCR and KPMG developed protocols for KPMG to follow in conducting these audits, but they have not been made public, which makes it difficult to prepare for the audit. CMS had conducted HIPAA security audits of 10 providers in 2008 and 2009, which may be of some benefit, although since OCR and KPMG have created new protocols, CMS’ older checklist may not be complete. “It’s a whole new process,” McDavid explains. (For a more recent HIPAA privacy and security rule checklist for documents and other information, see *MPCA 5/2/11*).

- **What are the consequences of an audit?** OCR says it intends to broadly share best practices in HIPAA compliance and provide guidance to the industry. Audited providers will have the opportunity to note in the final report corrective actions they’re taking to address issues KPMG finds during the audit. But if KPMG uncovers noncompliance, expect to incur fines and other penalties, notes Kline.

- **Who will be chosen to be audited?** OCR has indicated it will audit a broad spectrum of covered entities, but hasn’t shed additional light on who may be targeted or how OCR will choose. It may be related to particular problem areas OCR has identified or entities

OCR believes are at risk of noncompliance, says Kline. Since OCR will be auditing 150 entities, the audits will probably occur throughout the country, says McDavid.

However, while only 150 covered entities will be audited in this initial pilot, those who are chosen may be in for a rough ride. It’s likely that those audited will undergo a very detailed, burdensome audit, similar to tax audits conducted by the IRS in the 1990’s, another “random” audit program, which some called “nightmares,” warns Kline. “To test if taxpayers really had the dependants listed on their tax returns, the IRS wanted passports or birth certificates,” he notes.

What is clear is that this is uncharted territory for you and OCR, and it’s subject to change, says Kline. “What should providers be doing? What is the standard [of best practices] of each type of covered entity? This is a daunting task for everyone,” he points out. — *Marla Durben Hirsch* ([mhirsch@decisionhealth.com](mailto:mhirsch@decisionhealth.com))

#### **On the Internet:**

- ▶ HIPAA audit: [www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html](http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html)

## **RACs**

*(continued from pg. 1)*

Make sure your practice has also set up its billing forms to prompt for certain information based on what the auditors want, according to Pyles.

**Note:** Be careful not to wade into areas that could be considered fraud and abuse while still providing needed services to your patients, he says.

“Be mindful of the criteria – it’s not just a paper issue,” Pyles adds. “Most doctors just want to conduct their practice and provide services to patients without too much hassle.”

### **‘Another layer of potential problems’ for physicians**

The new demonstrations like prepayment reviews and prior authorization for certain medical equipment equals “more oversight” and “another layer of potential problems for physicians,” says Gregory Piché, proprietor of Singularity Health Law PLLC in Denver.

**Note:** The RAC prepayment review is focusing on problems that occur at the front end, Piché says. “No one looks at the front end.”

The RAC prepayment reviews can be seen as an extension of the Medicare Fraud Strike Force, which is very active in Florida and Michigan, Piché says.

**Example:** A pair of sisters in Michigan ran a fraudulent operation that was supposed to provide AIDS medication to patients, according to Piché. However, “the system was outdated and the sisters made out with millions from Medicare.”

**Note:** RACs will look at algorithms for areas that represent high levels of fraud or mistaken documentation, according to Piché.

**TIP:** Make sure your documentation is accurate with the CPT code and is sufficient to cover the requirement for payment for that code, he says.

“Make sure it’s in the file and your people are trained to handle it,” Piché adds.

### Make sure your documentation is in order

If a RAC asks for a sample of your records during a pre-payment review, that will hold up your payment, says Jodi P. Berlin, a partner with Hooper, Lundy & Bookman in Los Angeles.

**Note:** “It creates more of a paper issue – the office will have to submit more paperwork if claims are looked at for things such as medical necessity,” she says.

**TIP:** Keep a copy of everything you’ve submitted in case your claim is denied and you want to appeal, Berlin says. Ensure you submit proper and accurate claims and sufficient documentation for services that are ordered and rendered, she adds. “Make sure your coding is done properly ... and proper billing measures are in place.”

### Audit demos eyeing certain states

The RAC prepayment reviews will focus on seven states with a high population of fraud and error-prone providers, according to CMS information: **Florida, California, Michigan, Texas, New York, Illinois and Louisiana.** The RAC reviews will also focus on four states with high claims volumes of short, inpatient hospital stays: **Pennsylvania, Ohio, North Carolina and Missouri.** The other MAC demonstration announced by CMS will require prior authorization for certain medical equipment for all people with Medicare who reside in seven states with high populations of fraud and error-prone providers, agency officials said: **California, Florida, Illinois, Michigan, New York, North Carolina and Texas.**

Inform your staff of any record requests from an auditor and make sure those requests are processed through the proper channels, Berlin adds (*MPCA 11/15/10*). “Requests sometime go into piles and nothing is done.”

— Chris Huntemann ([chuntemann@decisionhealth.com](mailto:chuntemann@decisionhealth.com))

### On the Internet:

- ▶ RAC Prepayment review fact sheet: [www.cms.gov/apps/media/press/factsheet.asp?Counter=4170](http://www.cms.gov/apps/media/press/factsheet.asp?Counter=4170)
- ▶ Prior Authorization fact sheet for certain medical equipment: [www.cms.gov/apps/media/press/factsheet.asp?Counter=4168](http://www.cms.gov/apps/media/press/factsheet.asp?Counter=4168)

## delay

(continued from pg. 1)

too difficult to guess what OESS is looking for. OESS would want evidence that practices are in the process of adopting and using the new standards, including:

- Meeting the requirements for version 5010, such as using the 9-digit zip code in the address loop.
- Installation of the software upgrade, or evidence that the installation is in process such as communications with the vendor.
- Testing the upgraded system with payers.
- Training of staff in the new system.

**Stay tuned:** The situation may get even more dicey. The upgrade from the ICD-9 diagnosis and procedure codes to version ICD-10 will be an even bigger effort on the part of plans and providers, since this entails more changes. That transition is slated to occur Oct. 1, 2013. Implementation of version 5010 is a prerequisite for using the updated ICD-10 codes.

The American Medical Association (AMA) voted Nov. 15 to “work vigorously” to stop the implementation of ICD-10, according to an announcement the same day. The American Health Information Management Association (AHIMA) responded by saying the change was inevitable and to delay would only add additional costs.

There may be a showdown yet. — Marla Durben Hirsch ([mhirsch@decisionhealth.com](mailto:mhirsch@decisionhealth.com))

### On the Internet:

- ▶ 5010 delay announcement: [www.cms.gov/ICD10/Downloads/CMSStatement5010EnforcementDiscretion111711.pdf](http://www.cms.gov/ICD10/Downloads/CMSStatement5010EnforcementDiscretion111711.pdf)



From the  
**DECISIONHEALTH® PROFESSIONAL SERVICES**  
**Case Files**

**Case 72: The case of the ‘recycled’ PHI**

**The client:** A mid-sized single specialty practice in the Southwest.

**The audit:** Random chart audits for compliance with applicable billing rules.

**The audit result:** Our audit found a fairly high rate of success with the claims submitted by this practice. But it was something else that caught our attention and placed this practice at a high risk. While on-site reviewing the charts, the auditor went to recycle paper and noticed, in plain sight, patient protected health information (PHI) printed on paper that had been thrown into the recycling bin. The bin was unattended and, upon asking people at the practice, the auditor was told the recycling bins were emptied “when they got to be full.”

**Lessons learned:**

- **Exposed PHI places the practice at high risk for HIPAA violations and must be secured or shredded after every business day.**

The auditor concluded, based on the responses from practice staff, that it was not unusual for recycling bins to sit in unsecured areas and not be emptied or the contents secured for days at a time.

When PHI is placed in a recycling bin, then left unattended by the practice’s staff, it is not any different from leaving it on a desk or other area. When your office is cleaned at the end of the day by an outside cleaning service, any of those people could easily steal the documents from the recycling bin and use them as part of a patient identity theft scheme (*MPCA 7/11/11*).

- **Put a policy in place to handle the disposition of materials placed into paper recycling bins with accountability for follow-up.**

Any recycling bins at risk for containing patient PHI need to be emptied at the end of each business day. In order to ensure the security of the contents of the bins, plan to either shred the documents at the end of the day, or place the contents into either a secured area or a locked shredding bin.

**Note:** Access to these areas must be controlled to ensure that they are truly secure.

Sean M. Weiss, vice president & chief compliance officer of DecisionHealth can be contacted directly at [sweiss@dhprofessionalservices.com](mailto:sweiss@dhprofessionalservices.com) or at 1-301-287-2208. DecisionHealth Professional Services provides full-scale medical consulting services. To learn more about our services visit us at [www.dhprofessionalservices.com](http://www.dhprofessionalservices.com) or contact us at 1-888-262-8354.

Please pass this coupon to a colleague who could benefit from a subscription to *Medical Practice Compliance Alert*.

**YES!** I want news and guidance to help me stay on the right side of health care fraud, abuse and other laws and regulations. Please enter my one-year (24 issues) subscription at \$547. This includes access to the electronic version.

Name: \_\_\_\_\_  
 Org.: \_\_\_\_\_  
 Address: \_\_\_\_\_  
 City/State/ZIP: \_\_\_\_\_  
 Phone: \_\_\_\_\_  
 Fax: \_\_\_\_\_  
 Email: \_\_\_\_\_

**Payment enclosed.** Make checks payable to *Medical Practice Compliance Alert*; (TIN: 26-3622553)

Send me an invoice (PO \_\_\_\_\_)

Charge my:        

Card #: \_\_\_\_\_ Exp. Date: \_\_\_\_\_

Signature: \_\_\_\_\_

Mail to: **Medical Practice Compliance Alert**

Two Washingtonian Center, 9737 Washingtonian Blvd., Ste. 100,  
 Gaithersburg, MD 20878-7364 | 1-855-CALL-DH1

[www.compliancealert.net](http://www.compliancealert.net)

PAS 2011

## SIUs have a lot of power and aren't afraid to use it

A lot of physicians believe fraud investigations launched by private payers are less important than those from the government. That would be a mistake. While it's true a special investigations unit (SIU) can't bring criminal charges against your practice, SIUs still wield a big compliance stick, says attorney Stephen Sozio, with Jones Day in Cleveland (*MPCA 11/14/11*). Private payers can still withhold payments, use offsets to recoup money you owe and terminate your contract, says Loretta Worters, vice president of the Insurance Information Institute in New York City.

"SIUs have a lot of bullets in their chamber and will fire as many as they need," says James Quiggle, director of communications, Coalition against Insurance Fraud, in Washington, D.C.

In addition, SIUs usually inform law enforcement of their findings, so providers end up in the government's crosshairs anyway. Blue Cross and Blue Shield of Georgia recovered \$4 million in 2011 after its SIU conducted an investigation, including undercover activity, against a string of chiropractic offices, and eventually turned the case over to the U.S. Attorney's Office for indictment. The payer received an award from the payer industry in May for its efforts.

SIUs also testify at providers' sentencing hearings. "I put it into dollar terms. One doctor recently stole \$2 million. I testified how many pediatric electric wheelchairs and dialysis treatments that could have covered," says Alanna Lavelle, Blue Cross and Blue Shield of Georgia's Director of Special Investigations, in Atlanta.

Their scope can also be broader than an investigation conducted by the government. SIUs often target billing improprieties involving procedures they cover that Medicare and Medicaid don't, says Sozio.

Moreover, private payers are increasingly willing to pursue providers in court for recoupment of overpayments they made due to the providers' fraud. "The potential of a large recovery [from a lawsuit] sends a powerful statement that trying to defraud that insurer is a dangerous game," says Quiggle.

**Example:** Allstate Insurance Company filed a lawsuit in August seeking to recover \$5 million against a physician, five

professional corporations and several others for fraudulent medical billing. The lawsuit was filed following an investigation by Allstate's SIU, according to the insurer's Aug. 23 press release. The fraud suit is Allstate's 31<sup>st</sup> filed against providers in New York state alone.

### Prepare yourself for possible investigation

Be prepared in the event you're the subject of an investigation by a private payer's SIU. Here are five tips to help you avoid or handle such an investigation:

1. **Bring the same rigor you apply to compliance with government billing to your private payer claims,** Sozio says. "Use best practices for all billing. It's not that much more effort; the rules are pretty much the same," he notes. Make sure you're using certified coders and coding books for these claims, according to Lavelle.
2. **Hire staff you can trust.** Check references and the HHS Office of Inspector General's exclusion database to make sure the employee hasn't run into billing trouble with the government or private payers in the past. "Conduct background checks to make sure an employee won't put your practice at risk," suggests Louis Saccoccio, executive director, National Health Care Anti-Fraud Association (NHCAA) in Washington, D.C.
3. **Check the payer's medical policies to make sure you're in compliance.** "Our policies are on our website. Claiming ignorance will not hold water," says Lavelle.
4. **Treat an SIU investigation very seriously.** Use an attorney when dealing with such an investigation to understand your rights and deal with the SIU effectively, Quiggle says. The SIU may have been investigating you for a while and probably already has evidence against you.
5. **Be honest and open about explaining discrepancies or issues.** If you have any information that justifies your billing, share it with the SIU. "If you resist, you're asking for records to be seized, floods of depositions, and other legal consequences," warns Quiggle. — *Marla Durben Hirsch* ([mhirsch@decisionhealth.com](mailto:mhirsch@decisionhealth.com))

## How did you get this email?

### Copyright notice

It is illegal to forward this electronic version of **Medical Practice Compliance Alert** to anyone else. It is a free benefit only for the individual listed by name as the subscriber. It's illegal to distribute electronically **Medical Practice Compliance Alert** to others in your office or other sites affiliated with your organization. If this email has been forwarded to you and you're not the named subscriber, that is a violation of federal copyright law. However, only the party that forwards a copyrighted email is at risk, not you.

To confidentially report suspected copyright violations, call our copyright attorney Steve McVeary at 1-301-287-2266 or email him at [smcveary@ucg.com](mailto:smcveary@ucg.com). Copyright violations will be prosecuted. And **Medical Practice Compliance Alert** shares 10% of the net proceeds of settlements or jury awards with individuals who provide essential evidence of illegal electronic forwarding of **Medical Practice Compliance Alert** or photocopying of our newsletter.

## QUICK COMPLIANCE QUIZ

### **Business Associates and Physician Fee Schedule**

---

Make sure everyone in your practice can recognize lax practices by your business associates and know the newest requirements in the 2012 Physician Fee Schedule. Many recent PHI breaches have been caused by a practice's business associates who have possession of PHI of the provider's patients and the new fee schedule has both added and dropped some requirements.

**Instructions:** Distribute this Quick Compliance Quiz to your staff and make sure they can identify subpar business associate practices and are familiar with the new information in the 2012 Physician Fee Schedule. **Suggested reading for staff:** *Medical Practice Compliance Alert*, October 31 and November 14 issues.

**1. True or False: Even if a practice's business associate causes a PHI breach, it's the practice's responsibility to report it.**

- True    False

**2. The Anti-Kickback statute applies only to services fundamentally paid for by \_\_\_\_\_ .**

- Medicare  
 Medicaid  
 Both Medicare and Medicaid  
 None of the above

**3. Practices that currently have an EHR vendor and wish to use the Physician Quality Reporting System (PQRS) should start talks with the vendor \_\_\_\_\_ .**

- If the PQRS can be installed at a discount  
 Now  
 Three days after deciding to use the system  
 A week after deciding to use the system

**4. True or False: An ordering doctor or non-physician practitioner (NPP) must continue to sign a requisition for clinical lab work.**

- True    False

**5. Fill in the blank: CMS removed developmental testing code 96110 from the list because the CPT 2012 manual replaces the word \_\_\_\_\_ with \_\_\_\_\_ in the descriptor.**

- Exam; modifier  
 Test; exam  
 Screening; exam  
 Testing; screening

# Answers

---

## 1. True

**Teaching moment:** The covered entity is required to report a PHI breach, even if it's caused by a business associate. "The covered entity, which is also the victim, is the name that's remembered," says attorney Michael Kline with Fox Rothschild in Princeton, N.J.

## 2. Both Medicare and Medicaid

**Teaching moment:** Some states like Massachusetts have their own statutes that also apply to private payers, according to Thomas S. Crane, a member of Mintz, Levin, Cohn, Ferris, Glovsky and Popeo P.C. in Boston.

## 3. Now

**Teaching moment:** The vendor may have a very narrow window of time in which to self-nominate. According to CMS, it will be no later than Dec. 31, 2011.

## 4. False

**Teaching moment:** CMS initially put the rule on hold after members of the health care community reacted negatively to the idea in the 2011 Physician Fee Schedule. Now the agency says it will not require the ordering doctor or non-physician practitioner to sign a requisition for clinical lab work.

## 5. Testing; screening

**Teaching moment:** In the Stark list, that code has been replaced with **G0451** (developmental test with an interpretation and report).