Medical Practice Compliance

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

ALERT

November 1, 2010 | Vol. 22, Issue 21

IN THIS ISSUE

New self-disclosure protocol no panacea for providers

You're still on uncertain ground for how to proceed when you discover a Stark violation despite CMS' new Voluntary Self-Referral Disclosure Protocol, published and effective Sept. 23 *(MPCA 10/18/10)*. The new protocol raises almost as many questions as it answered, experts say.

The new protocol was required by the Patient Protection and Affordable Care Act (PPACA). It does provide needed guidance and gives CMS the authority to settle Stark violations for less than the actual amount owed, according to attorney Andrew Wachler, with Wachler & Associates, Royal Oak, Mich. It also enables you to resolve the matter even if a whistleblower has surfaced regarding the violation, and buys you more time to repay any overpayment.

But it doesn't offer as much guidance as was hoped for, and until it's tested, be reluctant to use it.

*(see **protocol**, pg. 4)*

How to handle patient badmouthing of your practice on the Internet

Your patients are increasingly turning to social media – such as physician rating sites, blogs, and even Facebook – to share their opinions of the physicians who treat them. This exchange of information can be very helpful. But information posted is often negative – and how you react can open your practice to compliance risks.

"This is not a new problem. Patients often shared negative information by word of mouth. The delivery [via social media] is just a new, more public way of doing it," notes attorney Tobias Butler, a technology attorney and social media consultant in Atlanta.

Once the domain of the hotel and restaurant industries, the use of rating sites and other social media to share one's experiences is spreading into the health care industry. There are currently more than 50 sites that rate physicians and they're growing in popularity, according to Joy Tu, director of strategic partnerships and marketing

*(see **badmouthing**, pg. 5)*

Eliminate, reduce compliance risks by effective handling of detected offenses

It's important you have mechanisms in place to discover your own potential billing and privacy problems as well as anything else that could draw investigators, such as internal auditing programs and ways for employees to report concerns. What may be even more critical is how you deal with compliance issues once they've been brought your attention.

Having a defined process to respond to a problem is one of the seven core elements of an effective compliance program, according to the HHS Office of Inspector General's (OIG's) current Compliance Guidance for physician practices.

Unlike your internal auditing, which should be conducted on an ongoing basis, responding to discovered compliance problems will be sporadic, depending on when one pops up – and you need to be prepared to handle them as they occur, according to Wayne van Halem, president, the van Halem Group, Atlanta.

"What's important is that once a problem is identified, something is done about it. If an offense is detected and nothing is done about it, it negates the whole purpose of having a compliance plan [and will be worse than not knowing about the problem]," he explains.

You're now required to implement a compliance program under health reform and it's expected that you'll be told to base your plan on the OIG's existing Compliance Guidance and include the seven core elements, according to the proposed rule addressing these mandatory compliance programs published Sept. 23 *(MPCA 10/4/10)*.

How to conduct an investigation

Once an offense is detected, investigate to see if it's credible. Don't avoid investigating or do a lackluster investigation because you're not sure how to do it properly. Unfortunately, there is no exact science to conducting an investigation. "How to investigate is unique to the offense, so there are different investigations," notes van Halem.

What does appear to be universal: You or the people who conduct the investigation will likely need to both interview staff and others involved, witnesses, coworkers and supervisors, as well as a review any documentation related to the issue, such as audit reports, medical records and incident logs.

"You have to ask questions and find out what happened," says David Zetter, president of Zetter Health-

Subscriber Services

Editorial:
Scott Kraft – 1-301-287-2361 *skraft@decisionhealth.com*
Marla Durben Hirsch – 1-301-299-6155 *mhirsch@decisionhealth.com*
Sean Weiss – vice president, DecisionHealth Professional Services
sweiss@dhprofessionalservices.com

Marketing:
Elise Yore – 1-301-287-2274 *eyore@decisionhealth.com*

Subscriptions:
For direct questions about newsletter delivery and account status, please contact DecisionHealth® at 1-877-602-3835, or email us at: *customer@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-l*, 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*.

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

care Management Consultants in Mechanicsburg, Pa. who trains physician offices in compliance. van Halem suggests that compliance personnel, who are usually the personnel tasked with conducting the investigation, take a course on interview techniques.

Your investigation should determine the nature of the problem, its scope, its frequency, the duration, and the potential financial magnitude, according to the OIG's compliance guidance. Identify the cause of the problem, says van Halem.

"It could be a rogue employee, an ambiguity in a policy, or a vulnerability," van Halem points out. Check the individuals' understanding of the laws, rules and regulations, the adequacy of the training and competency of those performing the functions at issue (such as billing or IT). Determine whether the people involved acted intentionally or recklessly, and the nature and extent of potential liability of employees or your practice.

How to correct the detected offense

Once you uncover an offense, correct it and take steps to prevent it from reoccurring *(MPCA 4/5/10)*. The OIG wants you to create and implement a "corrective action plan." As with the investigation itself, the content of the corrective action plan will vary, based on what was uncovered and what steps you need to take to correct the problem. **Example:** You may need to report and repay an overpayment, discipline an employee and/or conduct training.

The OIG wants your corrective action plans to include, at a minimum:

- action to be taken
- person(s) responsible/accountable for implementing the action
- when the action is to begin
- when the action is expected to be completed
- objective measures that will demonstrate the implementation of the action.

An effective corrective action plan should also include ways to avoid and prevent this problem in the future, and assign someone to monitor the follow up activity, says van Halem. Having a good corrective action plan will help you reduce the risks associated with the problematic activity.

TIP: Create new policies to address the problem, says Donna Beaulieu, compliance officer, Quality Physician Services, Stockbridge, Ga., who regularly adds protocols to deal with issues that had arisen so there's a procedure should it occur again.

TIP: Add/update unrelated procedures to deal with compliance issues in general. **Example:** Start conducting exit interviews of employees leaving the practice, to uncover issues they may be aware of and correct them, says Zetter.

What to do when you disagree with your consultant

You may decide engaging a consultant is one strategy you can use to establish compliance programs, conduct a billing audit or other activities designed to optimize your performance. But when you disagree with the consultant's findings, it is a discrepancy you cannot take lightly.

"Consultants are paid to share their insight and knowledge, and that comes from years of experience working in a particular field," says consultant Wayne van Halem, president, the van Halem Group, Atlanta. "[However], there are good consultants and bad consultants and you may get conflicting information," he points out *(MPCA 3/8/10)*.

Sometimes even good consultants make mistakes, points out Sean Weiss, vice president of DecisionHealth Professional Services and chief compliance officer of DecisionHealth.

"There are also gray areas in the business and regulatory aspect of health care that are subject to differing interpretations for coding, billing, regulatory and other items," notes Weiss. The policies and regulations are complex and convoluted, lending themselves to differences in interpretation, notes van Halem. The Medicare Administrative Contractors (MACs) often don't even agree with each other, points out consultant Day Egusquiza, president, AR Systems, Inc, Twin Falls, Idaho. Weiss estimates providers disagree with their consultants about 15%-20% of the time.

However, when the consultant has pointed out a compliance problem and you ignore it, your knowledge of it can increase your liability when

it turns out the consultant's advice was correct, warns attorney Gerald "Jud" DeLoss, DeLoss Health Law, Deerfield, Ill. You're responsible for your own actions, reminds Weiss.

There's a difference between merely disliking the consultant's findings because they're unfavorable to your practice and disagreeing with them because you believe they're wrong or your interpretation is plausible.

Here are four tips to help you determine your next actions when you disagree with your consultant:

1. Ask for verification – and verify your own position. Your position may be based on information from another consultant who had provided the practice with incorrect or partial information. That is something you need to double check, notes Weiss. Also, verify the current consultant's position. All positions/interpretations should be supported by written policies, regulation, or other authority. If there's still a disagreement, go directly to the government. "We always send [clients] to their MAC for clarity. There really is only one right answer and that is CMS and your MAC," says Egusquiza.

2. Get another opinion. If the difference in interpretation is not one where you can easily obtain an official government position, get a second opinion from another consultant, suggests van Halem.

3. Get a confidentiality promise in writing. Make sure you have a written contract with the consultant and it contains a confidentiality clause. "The clause should limit the consultant from releasing information except when required by legal action, such as a subpoena," says van Halem. Most consultants don't turn in their clients, particularly over what may amount to a reasonable difference in interpretation. But having the confidentiality clause may serve as a deterrent to keep a disgruntled consultant from going to the government. The confidentiality clause protects you by allowing you to claim the consultant violated your agreement.

4. Claim attorney-client privilege. Consider having certain functions, such as chart audits, be conducted under the auspices of attorney-client privilege, which gives any discoveries and advice added protection from government or other scrutiny, suggests Weiss.

protocol

(continued from pg. 1)

Three problems with the new protocol include:

• **It does not distinguish between technical and substantive Stark violations**. Groups representing your interests had asked CMS to take a two-track approach, where technical Stark violations (such as a contract that wasn't signed or had inadvertently expired) would result in expedited reviews and more modest penalties. The protocol doesn't differentiate, which means the punishment for technical, unintentional Stark violations can be disproportionate to the intent and extent of the violation itself. "The punishment doesn't fit the crime. [Almost] everyone has technical violations of the Stark law," says Wachler.

• **CMS has no obligation to settle the Stark violation for less than the full amount owed and the protocol does not identify when CMS would do so or how it might calculate any reductions**. In contrast, the OIG's self disclosure protocol, which applies to self-disclosures of violations of the anti-kickback law (and of the Stark law only if there's also an anti-kickback law violation), bases the penalties in part on the amount of money involved, so you can better weigh the benefits of self disclosure and the amount the OIG may settle for. "It's almost a benefit to have both an anti kickback and a Stark violation, because then you have a sense of the amount of penalties that will be assessed," notes attorney Lawrence Conn, with Foley & Lardner, Los Angeles.

• **CMS may still share your disclosure with law enforcement**. The new protocol applies only to violations of the Stark law. If you're dealing with potential violations of other laws, such as the False Claims Act or the anti-kickback statute, the new protocol doesn't help you. The anti-kickback violations would need to be disclosed via the OIG's protocol. Worse, the protocol makes it clear CMS may share your disclosure with law enforcement, so other agencies may still come after you, warns Conn. In contrast, the OIG's self disclosure law for anti-kickback violations allows the OIG to share the disclosure with law enforcement, but you can request that law enforcement join the provider and the OIG in the settlement discussions.

"It really puts people in a quandary. PPACA had clear language to repay an identified overpayment,

so if you identify a Stark violation, it's hard to ignore it," warns Conn.

Actions for your practice to take

You can't ignore the new protocol despite its problems. Here are five steps for your practice to take:

1. Review your contracts and relationships to ensure they are Stark-compliant. If you uncover a Stark violation, correct it going forward, says Wachler.

2. If you identify a potential Stark violation, explore all angles to see if you have any arguments that the relationship is legitimate. **Example:** The relationship may fall within a Stark exception that you hadn't considered, suggests Conn.

3. Weigh whether you have another disclosing option that has more of a track record. If you (and your attorney) believe you'd be better off disclosing a possible violation of the law to the OIG or the U.S. attorney's office and the nature of the violation would permit you to do so, consider that possibility, says Conn.

4. Have your attorney anonymously explore with CMS how it would treat you should you disclose your violation under the new protocol. At least that way you have a better idea of what to expect. Once you disclose, you're stuck, notes Wachler.

5. Consider incorporating into your compliance program factors that CMS will take into account when deciding how lenient to be. **Example:** Since CMS will look favorably at the extent you cooperated and how quickly you self-disclosed a violation, you may want to add or emphasize such factors, as well. "It helps put you in the best situation possible," says Wachler.

To view the new CMS Protocol, go to: *www.cms.gov/PhysicianSelfReferral/Downloads/6409_SRDP_Protocol.pdf*

To view the OIG self disclosure protocol, go to: *http://oig.hhs.gov/authorities/docs/selfdisclosure.pdf*

badmouthing

(continued from pg. 1)

for Medical Justice, a physician advocacy company based in Greensboro, N.C.

The rating systems include physician-only rating sites such as rateMDs.com, general sites that include physician services as categories, such Yelp or Angie's List, and private rating sites operated by health plans.

"The public sites are open sourced, so anyone can post and review, and it's often done anonymously," says Tu. Some of the rating sites allow patients to assign number ratings to the physician; others enable patients to add comments about the service provided, costs, waiting times, and the like. Some sites are moderated and provide services in addition to physician rating, such as a physician finder and lists of their credentials. Some don't police or monitor their sites at all. "[Some of this] is like the wild wild west," she notes.

In addition to rating sites, patients and others can badmouth you on a list serve, blog, YouTube, or other social media outlet. Even the members-only rating sites of private payers are accessible by thousands of people.

Because the information is searchable and public, a negative post or rating can be devastating to a practice's reputation – and could negatively affect its bottom line. It also creates potential problems for your practice, including:

- **HIPAA violations**. Social media communications dealing with protected health information (PHI) are subject to HIPAA. So when you attempt to defend yourself by responding online to a negative comment, you could end up violating HIPAA, warns Butler. **Example:** If you refute a negative assertion about the care you provided to a patient who posted on an online forum by posting PHI, posting information that may identify the patient or even saying HIPAA bars you from publicly responding to the unfounded complaint, you could be violating HIPAA's privacy rule. You could argue the patient opened the door to responses by posting in the first place, but this is untested territory and it is the providers who are subject to HIPAA, not the patient. "You don't want to be the test case," Butler adds.
- **State privacy law violations**. Some state privacy laws are more restrictive than HIPAA, permitting no disclosure whatsoever. Unlike HIPAA, which provides no private right of action against a violator, state laws often allow the patient to sue the physician directly.
- **Medical malpractice**. You always run the risk of being sued by a patient for malpractice. Some responses may increase your risk. **Example:** If you respond on-line to a negative post by saying "I didn't offer the more expensive treatment options because

(continued on pg. 8)

From the
DECISIONHEALTH® PROFESSIONAL SERVICES
Case Files

Case 46: The case of the serial undercoders

The client: A small practice in the Southeast

The audit: DecisionHealth Professional Services was hired to perform chart audits for a small primary care practice, including both physicians and non-physician practitioners (NPPs). The practice billed some E/M claims using time-based billing, but the majority of the claims were billed using history, exam and medical decision-making.

The practice had concerns that it might be overcoding services in some cases and definitely wanted to get a baseline sense of its overall E/M performance. The results were surprising. We found two providers at the practice consistently undercoded E/M services far more than any services in the entire audit were overcoded.

While audit reports in the Comprehensive Error Rate Testing (CERT) program, Recovery Audit Contractor (RAC) audits and reports from the HHS Office of Inspector General (OIG) regularly raise concerns about overcoding, your practice can also face scrutiny for consistent undercoding because it is still incorrect billing and opens you to accusations of cutting favorable deals for your patients in order to encourage repeat business.

Even though the majority of audits and investigations uncover more examples of overcoding, auditors do regularly spot undercoding.

The background: When an E/M service is based on history, exam and medical decision-making (MDM) for an established patient (**99211-99215**), you base your code selection on two of those three elements. As the code intensity rises, the mandate is that you do more intense work for that history, exam and MDM.

When billing for a new patient (**99201-99205**), your billing needs to factor in all three of history, exam and MDM. In addition, the lower codes in the code series for new patients often require more intense documentation than their established code counterparts because when it's a new patient, there is no established relationship between the patient and the provider.

Most experts will tell you that you can always create detailed documentation for most paper encounters if you choose. Two examples are reviewing and documenting systems not related to the patient's presenting problem or doing a comprehensive or detailed examination of a patient that includes an excessive focus on areas unrelated to the reason the patient came into your office.

You can do those things, but most auditors will tell you they are not justified. In Medicare Claims Processing Manual, ch. 12, sec. 30.6.1, CMS says: "Medical necessity of a service is the overarching criterion for payment in addition to the individual requirements of a CPT code. It would not be medically necessary or appropriate to bill a higher level of evaluation and management service when a lower level of service is warranted. The volume of documentation should not be the primary influence upon which a specific level of service is billed. Documentation should support the level of service reported."

It is the language that specifically cites medical necessity that sometimes has the opposite effect – it causes the practice to bill for a service that is less than it deserves just to ensure it can be justified on an audit, or to be on the safe side and try to avoid the audits.

That was what happened in this audit – when we reviewed the medical records for two of the provid-

Case Files

(continued from pg. 7)

ers, there was a pattern of services documented that supported a level of service that was one-level higher than the service actually billed by the practice.

In fact, the error rate in the audit for these two providers was nearly 40%, with more instances of undercoding than overcoding. In each case, we were able to establish based on the available documentation and interviews with the providers that higher-level services were justified by the medical records.

When we discussed our findings with the providers, they said that whenever they had a doubt about which code to select, they simply opted to select the lower code because each figured it would decrease the odds their claims would be selected for a government or private payer audit. Because of this coding philosophy, we found virtually no instances of overcoding by either practitioner.

Recommended Corrective Action Plans: We reviewed the 1995 and 1997 E/M guidelines with each practitioner, and emphasized the importance of choosing a level of service based on the work done and documented, both to bill compliantly and to ensure the practice collects the revenue to which it is entitled.

We shared scenarios with each provider, and explained why the provider could confidently bill higher level services in those scenarios based on medically necessary documented work.

We showed the practice Medicare billing data which showed that billing patterns for these two providers were well below the national average for the specialty, and explained that auditors would also review this data and could select the practice for an audit. Worse, a pattern of undercoding could suggest the practice was cutting deals for patients.

On the Internet:

- Medicare Claims Processing Manual: *www.cms.gov/manuals/downloads/clm104c12.pdf*

Sean M. Weiss, vice president & chief compliance officer of DecisionHealth can be contacted directly at *sweiss@dhprofessionalservices.com* or at 1-770-402-0855. DecisionHealth Professional Services provides full-scale medical consulting services. To learn more about our services visit us at *www.dhprofessionalservices.com* or contact us at 1-888-262-8354.

(continued from pg. 5)

she wouldn't have paid for it," or even "my office staff was only rude because the patient was nasty when he walked in," you're now on record for having said that and it can be used against you.

• **Defamation**. If the patient has acted truthfully but your physician's response is not accurate, the physician can end up being the defendant in a defamation claim, warns attorney Gerald "Jud" DeLoss, DeLoss Health Law, Deerfield, Ill. "Truth [of what the physician says in response] is a defense; however, establishing the truth or falsity to any statement is an expensive and time consuming process," he points out.

• **Malpractice insurance problems**. Medical malpractice insurance underwriters use rating sites to help determine a physician's insurability and the cost of the insurance, says Jeffrey Cutler, vice president of Business Development and Online Partnerships for Lyndhurst, N.J.-based Vitals.com, one of the most comprehensive physician locator and rating sites.

• **Managed care contract problems**. Some private payer contracts may limit or bar providers from retaliating against a patient complainer. Challenging a negative post or taking other action against the bad-mouthing patient, even in private, may violate your contract, warns DeLoss.

• **Escalation**. A public response to a negative comment or rating can create more negative posts from the patient on that site and other social media outlets. The patient may even be incensed and start contacting the state medical board and/or the Better Business Bureau. Even if you've done nothing wrong, you're now in a worse situation than before.

Many rating sites won't remove a patient's negative post, even if you believe that the information is frivolous or fabricated. **Example:** Vitals.com won't take down negative posts, although it will allow physicians to hide two of them, says Cutler.

Your practice can't afford to ignore these ratings sites and the fact that you're being talked about online. "Physicians must learn to adapt to it. This will grow, so learn from other industries [where this is already prevalent]. Your circle of who to listen to is getting bigger," says Butler.

Next issue: 10 strategies to protect your practice from patient badmouthing on the Internet.

Quick Compliance Facts

• **CMS warns physicians to improve their billing of pharmaceutical injectables**. CMS issued guidance in October warning doctors that the Recovery Audit Contractor (RAC) program has detected a large number of billing problems regarding pharmaceutical injectables. The problems included incorrect coding of the injectables, billing for excessive or multiple units, billing for medically unnecessary injectables and duplicate claims. CMS suggested physicians review the Medicare Claims Processing Manual, ensure staff is aware of Medicare policy on billing for drugs, and adequately document a physician's drug orders, dosage administered and, where required, dosage wasted amount. The guidance can be viewed at *http://www.cms.gov/MLNProducts/downloads/MedQtrlyComp_Newsletter_ICN904943.pdf*.

• **Medicaid RACs one step closer to implementation**. The expansion of the Recovery Audit Contractor (RAC) program to Medicaid, required by the Patient Protection and Affordable Care Act enacted in March, is now underway. CMS has sent guidance to state Medicaid directors regarding how to create Medicaid RAC programs and has required them to attest that they will establish a Medicaid RAC program (or indicate that they will be seeking an exemption) by December 31, 2010. The guidance, sent October 1, also outlines how the state Medicaid agencies shall contract with and pay these new RACs and warns states they can't supplant existing state program integrity or audit initiatives with Medicaid RACs.

• **OIG allows free preauthorization services by radiologists for other physicians**. The Office of Inspector General (OIG) reiterated its tolerance of providers offering free insurance authorization services to referring physicians, this time offered by other physicians. In facts similar to those presented by a hospital seeking to provide these services *(MPCA 10/4/10)*, the OIG said in an advisory opinion posted September 28 (No. 10-20) that it would not sanction a radiology group that wished to offer free preauthorization services to referring physicians. The OIG said that the radiologists had a legitimate business interest in obtaining the preauthorization from the referring physicians. The OIG also noted that the arrangement had a low risk of fraud because the service will be offered to all physicians, the program would be transparent, and no money would be changing hands. To view the advisory opinion, go to *www.oig.hhs.gov/fraud/docs/advisoryopinions/2010/AdvOpn10-20.pdf*.

How did you get this email?

Copyright notice