Medical Practice Compliance
News, tools and best practices to assess risk and protect physicians
ALERT

February 18, 2013 | Vol. 25, Issue 3

MCA 2053931204 Copies 1

MICHELLE M LOTT
WASHINGTON STATE MED ASSOC
2033 6TH AVE STE 1100
SEATTLE, WA 98121-2585

IN THIS ISSUE

Sunshine Rule final; clock ticking on disclosure of vendor payments

The final rule implementing the Sunshine Act requires most payments and goods valued at greater than $10 that physicians receive from pharmaceutical and medical device manufacturers to be posted on a public website.

The rule requires these manufacturers as well as group purchasing organizations, including physician-owned distributorships, to track and annually report to HHS payments, gifts and other "transfers of value" of $10 or more and "ownership and investment interests" they provide to physicians and teaching hospitals.

Data collection starts Aug. 1 and ends on Dec. 31 for 2013; the manufacturers must report those payments by March 31, 2014. Thereafter collecting and reporting will be on an annual basis.

Published in the *Federal Register* Feb. 8, 2013, the rule, part of the Affordable Care Act, is designed to increase transparency in the financial dealings between manufacturers and providers.

Physicians under the magnifying glass

While the obligation to report — and penalties for failing to do so — falls on the manufacturers, the physicians will be the ones in the spotlight, since what they receive from manufacturers will be available for patients and others to see.

(SEE **BUSINESS RELATIONSHIPS**, P. 2)

Mega-rule protects patients from disclosure of self-pay treatments

One of the least publicized — but potentially most burdensome — obligations coming out of the new HIPAA "mega rule" is the requirement to hide from payers the fact that you treated a member if the member requests it and pays you in full for the treatment.

The original HIPAA regulations gave you the discretion to agree to restrict the disclosure of patient protected health information (PHI). But the Health Information Technology for Economic and Clinical Health (HITECH) Act created an exception. Now you are required to comply with patient requests that their PHI not be disclosed to a health plan for

(SEE **HIPAA**, P. 5)

CONTINUED FROM P. 1

Start logging payments from vendors now

BY **MARLA DURBEN HIRSCH**

Unfortunately, many physicians don't understand that they'll be under increased scrutiny and that these payments may call into question their objectivity when treating patients. A recent survey of more than 1,000 physicians by MMIS found that more than half of them didn't understand the law, notes Gary Keilty, managing director for Huron Healthcare's compliance and investigations practice, in Washington, D.C.

Expect them to start reacting once they get wind of it. "A large number of doctors will start dropping out of promotional and clinical programs. They won't want to be associated with these payments," predicts Manny Tzavlakis, managing director for the life sciences practice for Huron Healthcare in New York, N.Y.

Exceptions to the rule

There is some good news: Not every "transfer of value" is reportable. For instance, gifts of nominal value, such as pens, are not reportable, nor are samples or educational materials for patient benefit, such as anatomical models. Payments for a purely legal or administrative proceeding are also exempt from reporting.

The final rule also creates a loophole for speakers' fees: A payment is not reportable as an indirect payment if the manufacturer pays a continuing education provider, not the physician, and doesn't recommend or select the physician speaker. "This is huge. You can drive a truck through it. Manufacturers will try to get money to doctors through it," says Bennett.

Learn more:

- Read the rule: *http://tinyurl.com/agbota7*
- Read about the MMIS survey: *http://tinyurl.com/be2wea8*

What you need to know about the Sunshine rule

While such payments are not necessarily inappropriate, tread carefully, since this rule will have a big impact on you in eight key ways:

- **The reporting threshold is very low.** Any transfer of value of $10 or more must be reported. If your office accepts $20 worth of bagels and coffee from a manufacturer, it's reportable, says Mary Bennett, vice president of advisory services for consulting firm Novex Global in Mundelein, Ill.
- **The rule covers direct and indirect payments.** You can't direct the payment to someone not subject to the rule, such as your nurse practitioner, if she's going to turn around and give it to you. You also can't avoid the reporting if you designate the payment elsewhere on your behalf.
- **You don't have to consent to a gift for it to count as reportable.** For instance, if your nurse practitioner accepts textbooks from a manufacturer and doesn't tell you but puts them in your library, the books are reportable. "You can be on the hook without even knowing it," warns Bennett.
- **The public reports will be very detailed.** The information on the website will include your name, business address, specialty, state license number, date of payment, the amount, form and nature of payment (gift, consulting, entertainment, and the like).
- **You only get 45 days to dispute reported information and don't get to tell your side of the story.** Physicians have the opportunity to review the information that the manufacturer submitted to HHS before it's posted on the website. If the dispute is not resolved, the manufacturer's version is the one that goes on the website. All you get is a mark that indicates the payment is disputed.
- **Your patients and hospital affiliates may be checking up on you.** Patients' malpractice attorneys will be perusing the website to see if there are correlations between payments and their patients' injuries, trying to build their cases, warns Keilty. Hospitals which have instituted conflict of interest policies that ban or limit physicians' ability to accept these payments may check to see if you're in compliance.
- **Your payments will now be on the government's radar.** While many of these payments are for legitimate activities, expect them to be scrutinized by the government to see if they comply with the fraud and abuse laws, warns David Sclar, a health care attorney in the life sciences practice group of Cooley LLP in Washington, D.C. "It's an opportunity for the government to pursue them," he says.
- **Your reputation may be adversely affected.** These payments, especially large ones, will rile up patients and taxpayers, according to Bennett. "Anyone who gets a lot of money [from the manufacturers] will be called on the carpet for this," she warns. This can be particularly troublesome for a physician engaged in research, since the payment may be going to the research and not to the doctor.

Steps to comply with 'Sunshine Rule'

BY **MARLA DURBEN HIRSCH**

Many relationships between physicians and pharmaceutical and medical device manufacturers are valid and beneficial. But with the release of the final rule that makes payments between them public (*see story, p. 1*), you need to take these eight steps to reduce the legal and compliance risks stemming from the rule:

- **Review your contracts and relationships with manufacturers.** "These payments may all be valid but may can appear to influence [a physician]," says Mary Bennett, vice president of advisory services for Navex Global, in Mundelein, Ill. If you're not comfortable with one or more of them, take steps to unravel those relationships.

- **Make sure the relationships you do keep are legitimate and appropriate.** You'll want to be satisfied that you're in compliance with the fraud and abuse laws, says David Sclar, a health care attorney in the life sciences practice group of Cooley LLP in Washington, D.C. For instance, to avoid anti-kickback allegations, make sure you're being paid fair market value pursuant to a written contract.

- **Do your unraveling before Aug. 1 if you want to avoid reporting.** The reportable period begins Aug. 1, so if you terminate a relationship before then any payments made previously should remain private, says Bennett.

- **Keep track of all gifts and payments you receive.** Keep receipts and review 1099 forms. You'll want to have good records so that you can compare your information to that submitted by manufacturers and make sure that they're accurate, says Bennett.

- **Take advantage of the 45-day window to review the information that manufacturers report to HHS before it's posted.** "The onus is on the physician to make sure reports are correct," says Sclar. You'll need to register with CMS to gain access to this information once the agency makes that available.

- **Educate your staff about the rule.** They need to let you know if anything of value is coming into the practice, so you know whether to accept it, says Bennett. Also, patients will likely ask about payments you've received that they've seen on the website.

- **Know what the exceptions are.** Manufacturers may err on the side of caution and overreport payments arguably not reportable, such as an educational item for patient benefit, says Bennett. If you're not familiar with the exceptions, you won't know that you can dispute such reports.

- **Don't forget state law and applicable hospital rules that ban, restrict or require reporting of these payments.** "Many of these are not preempted by the new rule," warns Gary Keilty, managing director for Huron Healthcare's compliance and investigations practice, in Washington, D.C.

"To avoid anti-kickback allegations, make sure you're being paid fair market value pursuant to a written contract."

How to notify patients of a breach of their confidential information

BY **MARLA DURBEN HIRSCH**

The HIPAA "mega rule," published Jan. 25, 2013 in the *Federal Register*, finalizes the specific requirements covered entities must meet when notifying patients that a breach of their unsecured patient protected health information (PHI) has occurred (*MPCA 2/4/2013*). The rule implements the security breach notification requirements enacted by the Health Information Technology for Economic and Clinical Health (HITECH) Act.

The HITECH Act and the final "mega rule" are explicit about the form and content of a security breach notification to affected individuals. Generally, the notification needs to be in writing, plain English, and at an appropriate reading level. Because of other laws, such as the American with Disabilities Act or Civil Rights Act, you may need to send notification in large print or in other languages. There is no page limitation.

You would typically notify the patient by first class mail, to the patient's last known address; there are additional requirements for substitute notification or faster notification under certain circumstances, according to the rule. For instance, you may need to post notice of the breach on your website or in local media when more than ten of the addresses of affected individuals are found to be out of date.

The notification must include:

- A brief description of the breach, including the date of the breach and the date of its discovery, if known.
- The type of unsecured PHI affected, such as social security number and diagnosis.
- The steps the individual should take to protect himself from potential harm.
- What you're doing and have done to investigate, mitigate harm, and prevent future harm.
- Contact information, which must include a toll free number, email address, website, or postal address.

The HITECH Act requires notification to be made "without unreasonable delay" but in no event later than 60 calendar days after discovery of the breach.

Note: The final mega rule increases the likelihood you'll be notifying patients of such breaches, since there is now a presumption that you must notify patients of a breach unless after conducting a risk analysis there is a "low probability" that the data has been compromised, points out attorney Adam Greene, with Davis Wright Tremaine, Washington, D.C., speaking at a recent webinar. Previously, there was no such presumption.

However, while more security breach incidents will now be seen as reportable events, not every one of them will automatically fall within that category, since some of them will be of "low probability" that the information was compromised.

There are also a few limited exceptions where even a breach of unsecured patient data doesn't have to be reported, such as an unintentional good faith acquisition of PHI by a workforce member other than the intended recipient, says Mahmood Sher-Jan, with Idexperts, also speaking at the webinar.

Covered entities also don't have to conduct the risk analysis before providing notice; you can proceed directly to notification if you know the probability of compromise is more than "very low," points out attorney Kirk Nahra, with Wile Rein in Washington, DC speaking at another webinar.

> "You may need to send notification in large print or in other languages."

Learn more:

- Read the HIPAA mega-rule on the Federal Register at *http://tinyurl.com/bfyzgdy*

Mega-rule requirement places huge burden on providers

BY **MARLA DURBEN HIRSCH**

payment or health care operations if the services have been paid for out of pocket in full by the patient or someone else on his behalf, according to Sue McAndrew, Deputy Director, OCR, Health Information Privacy, at HHS, speaking at a legal conference explaining the mega rule.

Failure to comply with this provision of HIPAA's privacy rule subjects you to potential civil and criminal penalties. The mega rule, published in the *Federal Register* Jan. 25, goes into effect March 26; providers must comply by Sept. 23.

Physicians to bear brunt of new rule

While the provision applies to all providers, physician practices will end up with most of the burden, since that's where these requests will originate. Expect a higher percentage of these requests when you provide treatment of a more sensitive nature that a patient may not want in her record, such as sexual/pregnancy related treatment, or treatment that an employee may want to keep hidden from one's employer, such as diabetes, says attorney Elizabeth Litten, with Fox Rothschild in Lawrenceville, N.J. (*for a rundown of your new duties, see p. 6*).

What's worse is that the requirement will put physicians in a new, uncomfortable role, says attorney Michael Kline, with Fox Rothschild in Princeton, N. J. "It puts on a provider the responsibility to be a gatekeeper. It can create a conflict of interest since the patient is making decisions that affect a doctor's pay," warns Kline.

Providers do get one break, according to experts. You're not under any affirmative obligation to tell patients of this option, advises Litten.

"It's the patient's responsibility to bring it up. There's no need to wave a flag," she explains.

Questions left unanswered — including what to charge for treatment

Since this is a new consumer right, providers have no experience with it, and unfortunately the final mega rule still leaves a lot of unanswered questions, such as how to document compliance and how much a physician is supposed to "counsel" the patient about restricting disclosure. Example: It's uncertain to what extent a physician needs to point out how submitting a claim for part of a bundled service could affect the physician's reimbursement, says Litten. It also can strain your relationship with the patient if the patient doesn't pay you in full and you subsequently bill the plan.

It's also uncertain how much you can charge the patient for these out of pocket fees. You may be able to bill your usual charges and collect directly from patients, instead of the discounted rate you agreed to in a payer contract, says Litten. However, if you're in a state that limits your ability to charge more than the cost-sharing amount, you may be stuck

CONTINUED ON P. 6

"While the provision applies to all providers, physician practices will end up with most of the burden, since that's where these requests will originate."

Learn more:

- Read the HIPAA mega-rule on the Federal Register at *http://tinyurl.com/bfyzgdy*

New burden for providers

charging your discounted rate. You may even have to counsel HMO patients to go out of network, if they want the restriction, she points out.

The provision may also put a strain on the relationship between you and private payers. For instance, if the patient wants you to keep secret a particular treatment, that restriction may adversely affect your ability to get paid by a payer for follow up care, say if you hadn't obtained necessary precertification for the initial procedure, warns Litten.

"Physicians who already don't have enough time now have to be advisor and counselor on what it means to request the restriction," warns Kline.

Honoring patients' request to restrict information

Here's what you have to do to comply with the HIPAA " mega rule" that requires you to honor patient requests not to disclose to their payers (*see story, p. 1*):

- Flag or make a notation in the record to ensure that the information doesn't independently get sent to the health plan, such as during an audit. You don't have to segregate or create separate medical files for this restricted information.
- If a treatment is part of a bundled service, OCR expects you to counsel patients on the ability to unbundle it and the impact (i.e., the plan may glean the information from the remainder of the bundle being submitted by the provider for payment). If the requested restriction can't be unbundled, you're supposed to inform the patient and give him the chance to pay for the entire bundle out of pocket in full.
- Notifying "downstream" providers such as pharmacists or specialists about the restriction is not required, but you are "encouraged" to counsel patients regarding the need to contact those providers if they want the restrictions extended and "encouraged" to assist patients in alerting these downstream providers.
- If a patient is in an HMO and can't pay out-of-pocket for items other than cost sharing, such as copayments, you must tell the patient to go out of network.
- If the patient requests to pay directly to avoid an insurance claim, but hasn't yet paid out of pocket in full, you must make a "reasonable" effort to get payment from the patient before billing the plan.
- You need to add this new consumer right to your Notices of Privacy Practices (*MPCA 2/4/2013*).
- You must identify those employees who need to know about this provision and train them so that they can comply with the new requirement.
- If the patient receives subsequent related treatment and doesn't request a subsequent restriction, you can include the previously restricted information in accordance with the minimum necessary rules to the plan, but OCR "encourages" a dialogue between the provider and patient before doing so.

Learn More: There are several particularly important areas that impact physician practices in the recently released HIPAA mega-rule. Make sure you're fully prepared to meet them by joining compliance expert Frank Ruelas on March 13th for Expert strategies to update your practice's HIPAA compliance program. ***www.decisionhealth.com/conferences/A2358***

Subscriber information

EDITORIAL
Have questions on a story? Call or email:

Director of Content Management:
Scott Kraft, 1-301-287-2361
skraft@decisionhealth.com

Editor of Physician Solutions:
Karen Long, 1-301-287-2331
klong@decisionhealth.com

Editor:

Marla Durben Hirsch, 1-301-299-6155
mhirsch@decisionhealth.com

SUBSCRIPTIONS
Direct questions about newsletter delivery and account status, toll-free, to 1-855-CALL-DH1 or email to: *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.

Medical Practice Compliance Alert® is a registered trademark of DecisionHealth. DecisionHealth is a registered trademark of UCG. *Medical Practice Compliance Alert* is published 24 times/year by DecisionHealth, 9737 Washingtonian Blvd., Ste. 200, Gaithersburg, MD 20878-7364. ISSN 1047-1863. *www.decisionhealth.com* Price: $547/year.

CMS proposes to reduce 'burdensome' rules

BY **MARLA DURBEN HIRSCH**

CMS has issued a proposed rule to reduce some of your compliance burdens. Released Feb. 4, the rule aims to remove "unnecessary, obsolete or excessively burdensome" regulations, according to CMS. The agency says that the rule will save providers $676 million annually and $3.4 billion over five years.

While many of the suggested changes focus on hospitals, a number of them can have a significant impact on physician practices, including:

- Physicians who treat patients at "very small" critical access hospitals, federally qualified health centers or rural health clinics would no longer be required to be on site every two weeks.
- Physicians' obligations to supervise registered dieticians, technicians preparing radiopharmaceuticals and radiological services in ambulatory surgery centers would be relaxed and more flexible.
- Physicians would no longer have to be on a hospital's governing body.

This is the second rule issued to help providers operate more efficiently by getting rid of regulations that are out of date or no longer needed. The first such rule was issued May 2012.

CMS is accepting comments on the proposed changes for 60 days after its publication in the Federal Register, which is slated for mid-February. To read the rule and submit comments, go to *www.ofr.gov/OFRUpload/OFRData/2013-02421_PI.pdf.*

> "The agency says that the rule will save providers $676 million annually and $3.4 billion over five years."

News Briefs

- **Breach notification deadline March 1.** HIPAA's deadline for the reporting of "small" breaches (affecting fewer than 500 individuals) pursuant to the security breach notification rule is March 1, 2013. Small breaches of unsecured patient protected health information need only be reported to HHS annually. Larger breaches must be reported no later than 60 days after discovery of the breach. The notice of the breach must be submitted electronically, using HHS' online form. A separate form needs to be used for each breach. To access the form, go to: *www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.*
- **Government announces nearly 8:1 ROI on fraud recoveries.** The government has recovered a record $4.2 billion in fraud and abuse recoveries in fiscal year 2012, up from almost $4.1 billion in 2011, according to an announcement made by the attorney general's office and the secretary of HHS Feb. 11. For every dollar spent on investigating fraud, the government recovered $7.90, the highest three year average ROI in the 16-year history of the Health Care Fraud and Abuse Program. See more at: *www.hhs.gov/news/press/2013pres/02/20130211a.html.*
- **HHS moves forward in fraud info-sharing with payers.** HHS has taken another step in its efforts to work with private payers to reduce provider fraud by sharing data, delegating authority to CMS to consult with and arrange for data sharing with the plans. This project is part of the Health Care Fraud and Abuse Control Program. (*For more info see* MPCA 1/21/2013). Details at: *http://tinyurl.com/a4exj57*

Sample breach notification letter to patients

Here is a sample letter to alert patients of a security breach affecting their unsecured protected health information (PHI) (*see story, p. 4*). It covers the topics required by The HITECH Act and the final HIPAA "mega rule." If you also need to comply with a state security breach notification requirement, please incorporate those requirements so that you are in compliance with both federal and state applicable law.

This sample is intended to be general. You will need to customize it, based on the nature of the breach.

Via First Class Mail

Dear _____:

I am writing to you because we have learned of a data security incident that has occurred involving some of your personal information [describe what happened, when it happened, the date of its discovery, if known, and what type of unsecured PHI was breached].

We encourage you to take preventive measures to help prevent and detect any misuse of your information. We recommend that you place a fraud alert on your credit files, which tells creditors to contact you before they open any new accounts or make changes to your existing accounts. You may want to consider requesting a free credit report from each of the three credit companies. They are: Equifax, 1-800-685-1111, *www.equifax.com*; Experian 1-888-397-3742 *www.experian.com*, and TransUnion 1-800-916-8800, *www.transunion.com*. If any suspicious or unusual activity is noticed, you may want to contact local authorities and file a police report. [Add whatever additional protections you recommend. For instance, you may be offering free credit monitoring for a year or suggesting that the patients place fraud alerts on their accounts].

[Describe what you are doing to investigate the breach, mitigate losses, and to protect against any further breaches]

Should you have any additional questions or concerns, please contact us [use a toll free telephone number, email address, web site or postal address].

I apologize for any distress this situation has caused you and stand ready to assist you in any way. [if applicable], We have contacted the Department of Health and Human Services to alert it of this issue.

Sincerely,

_____

Source: Editor of Medical Practice Compliance Alert