Medical Practice Compliance

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

ALERT

October 2018 | Vol. 29, Issue 10

IN THIS ISSUE

5 compliance issues when dealing with private equity investment firms

BY **MARLA DURBEN HIRSCH**

Physicians are increasingly selling their practices to private equity (PE) investment firms. While these can be great deals, they also come with compliance risks for physicians.

A PE firm's acquisition of a practice is different from a hospital's acquisition of a practice, where the deal is construed as permanent and the physicians become employees of the hospital. In contrast, a PE firm typically is looking to invest in a practice, seeking to gain substantial control and sell its investment for more money in about five years. The physicians are still employed by the practice.

PE firms are jumping into health care, according to attorney Glenn Prives with McElroy, Deutsch, Mulvaney & Carpenter in Morristown, N.J. "There's untapped growth potential, and many practices don't operate efficiently," so there's the opportunity to increase efficiencies and be more productive, Prives says. These investments first began in

(SEE **BUSINESS RELATIONSHIPS**, P. 5)

10 ways to address human trafficking in your practice

BY **MARLA DURBEN HIRSCH**

There is no-one-size-fits-all way for a practice to respond when staff suspect or know that a patient is the victim of human trafficking (*MPCA 9/18*). It depends on the circumstances, the age of the victim, applicable reporting requirements, local resources and other factors, says Holly Atkinson, M.D., program director of human rights at the Icahn School of Medicine at Mount Sinai Medical Center in New York City.

It also may be hard to help a patient that you suspect is a trafficking victim, especially if they are afraid to accept help. They may be beat down, under a handler's lens, afraid of deportation and may admit it or refuse assistance. They don't need chains to tie them down, says Kelly Herron, director, Mission Services and Catholic Identity, Trinity Health in Livonia, Mich., speaking at recent American Bar Association's Health

(SEE **WORKPLACE COMPLIANCE,** P. 2)

DecisionHealth an H3.Group brand

100 Winners Circle, Suite 300, Brentwood, TN 37027 1-855-CALL-DH1

H3.Group a SimplifyCompliance business

CONTINUED FROM P. 1

Law Section conference. "If there isn't mandatory reporting, then you can only provide quality health care and support," Herron says.

However, practices should take these general steps:

1. **Make sure everyone in the practice receives training so they are familiar with the signs of human trafficking.** Anyone may recognize it, including the front desk or billing personnel, not just clinical staff. The Department of Health and Human Services has recently launched an online training module on human trafficking available for CME/CE credit. HEAL Trafficking, an organization dedicated to helping survivors, has developed a protocol toolkit for providers to adapt (*see resources, below*).

2. **Create a supportive environment for victims.** You can provide Human Trafficking Resource Center Hotline information and brochures from the National Human Trafficking Resource Center in private areas such as the bathroom and exam room, says Gomez.

3. **Try to speak with the victim in private.** If you suspect that a patient is a trafficking victim, try to get the patient away from the handler or companion and ask open-ended questions, such as "Are you safe? Are you hungry? Do you live, sleep and work in the same place? Are you OK?"

"You need to build trust and rapport. Survivors are concerned that they'll be judged and not listened to and are worried about confidentiality," says Jordan Greenbaum, M.D., with the Institute on Health Care and Human Trafficking, Children's Healthcare of Atlanta in Atlanta.

4. **If a patient discloses that he is a victim, offer him the hotline number (1-888-373-7888 or text 233733) so that the victim can seek help.** "You can't force them. It's up to the patient to take action," says Daniel Gomez, M.D, an ob/gyn in Fort Lauderdale, Fla., also speaking at the conference. If the patient doesn't want to take down the number for fear that a handler may find it on her person, help the patient memorize it or label it on a card so it looks like a referral to a health service.

5. **Know what local resources are available.** "If the victim discloses [that he is a victim of human trafficking], it's imperative to offer services in the community, such as crisis intervention and housing, not just health care," says Greenbaum. Other services to identify include legal aid, immigration assistance and social services. The hotline compiles this information and may have a list for your area so you don't have to do your own legwork.

6. **Be prepared to assist the victim in other ways.** A patient may need help even if she won't disclose that she's a victim or is not able or willing to take action. For example, you may want to discuss a safety plan with the patient, such as where could she go in the future. You might schedule a follow-up visit so that the patient needs to return. "It hits you hard. You can offer to help in the office but wonder what happens to the patient when she leaves the office. [A follow-up visit at least keeps the patient in touch]," says Gomez.

7. **Make sure you document what's legally required.** For instance, if the patient gave verbal authorization for you to disclose her information to a third party, such as a social services agency, make sure you put that into the medical record so you can show you complied with HIPAA.

8. **Use the hotline yourself for help.** For example, if you suspect a patient is a victim but he has not disclosed it or refuses help, you can still call the hotline with general, deidentified information and ask for advice.

9. **If you're in a state that mandates reporting, make sure that you report.** Note that contacting the Human Trafficking Resource Center Hotline will not necessarily fulfill this requirement; you'll need to see what your state requires.

10. **Be cognizant of the safety of the victim and of the practice.** "You don't know if it's a small ring or large organized crime [that's involved]," says Gomez. If the handler starts making threats, you may need to contact law enforcement, even 911.

RESOURCES:

- HHS' human trafficking training modules: *www.acf.hhs.gov/otip/news/soar-online*
- HEAL Trafficking's sample human trafficking protocol toolkit: *https://healtrafficking.org/2017/06/new-heal-trafficking-and-hope-for-justices-protocol-toolkit-for-developing-a-response-to-victims-of-human-trafficking-in-health-care-settings/*

Non-compete clauses may not bind; be sure to give the judge some leeway

BY **ROY EDROSO**

Question: *We have non-compete clauses in our doctors' contracts, saying when they leave us they can't practice within a certain radius of our offices for a certain period of time. But lately I've been noticing legal cases in the paper where doctors have challenged their non-competes and judges have released them. What were those practices doing wrong and how can we avoid it?*

Answer: Courts do regularly release providers from their non-competes, also known as restrictive covenants. But that doesn't mean the practices did anything "wrong" — it may just be that the judges felt their requirements were unreasonable. But you can take preemptive steps to limit the damage if they do.

First of all, not every state even allows restrictive covenants, and others have very clear radius and duration covenant restrictions.

But many state laws say these covenants have to be "reasonable," says Glenn P. Prives, attorney with McElroy, Deutsch, Mulvaney & Carpenter LLP in Morristown, N.J.

While most judges will look at what's common in the industry and base their idea of what's reasonable on that, what seems reasonable to you (and seemed reasonable to the provider when they signed the contract) may not meet with their approval.

"Generally courts do not want to [make it so that] an M.D. can't earn a livelihood," says Prives. "They don't want them to have to uproot their lives to make a living. There's a lot of case law out there siding with the complainant. I don't think you could put betting odds on it — but be prepared."

3 ways to make covenants stick

1. **Be careful how you draft it.** Have your lawyer look at it, of course, and use language and standards that make business sense. For example, says Prives, you should where appropriate make allowances for the provider's specialty. For example, says Prives, you should where appropriate make allowances for the provider's specialty. If the provider is a dermatologist, for example, where and for how long you could prohibit them to practice dermatology may vary from where and for how long they could practice general medicine, or a sub-specialty such as plastic surgery.

2. **Have blue pencil language.** Having your covenant thrown out could set a disastrous precedent for your practice. But if your agreement includes what's known as "blue pencil language" you could minimize the damage. Named for the editor's blue pencil in journalism, this language "acknowledges that if the court sees it as too broad, the court is authorized to narrow the covenant and enforce more narrow terms it deems appropriate rather than dispose of it entirely," says Prives. "For example, you may have three years/20 miles,' and they may say, 'not reasonable, but two years/10 miles is,' and they have the authority to impose that."

   But heads up: There *has* to be language in the contract that allows the court to do this, says Prives; "otherwise, the court must either enforce the covenant as written or have no covenant to enforce at all."

3. **Argue *your* right to a living.** When you get to court, argue that allowing the provider to compete for your business would hurt the practice. "Courts understand the need to protect your business interest," says Rives. "That's the reason to have restrictive covenants in the first place! They have agreed that they deserve that protection."

RESOURCE:

- Fox Rothschild guide to restrictive covenants: *www.foxrothschild.com/content/uploads/2015/05/National-Survey-on-Restrictive-Covenants-July-2017.pdf*

5 answers to common HIPAA questions asked by patients and practices

BY **MARY BRANDT, MBA, RHIA, CHE, CHPS**

Question: *I work for a large company. I called out one day because my daughter was sick. Do I have to provide a doctor's note to my employer when I wasn't the actual patient? I'm not under my employer's health plan.*

Answer: Your employer has the right to establish its own policies regarding employee absences and return to work. This is not affected by HIPAA or your health care coverage. As an employee, you are expected to comply with your employer's policies, and those policies may require you to provide written documentation of a doctor's visit for your child if you missed work for it. The doctor's office should provide this documentation on request and simply verify the date and time of your daughter's appointment. The documentation should not include any information on her medical conditions.

Question: *My daughter had to go out of town on business, and she asked me to make check-up appointments for her children. Our doctors are all at the same practice. The practice staff informed me that I am not permitted to make the appointments because of HIPAA. Is this really a HIPAA violation?*

Answer: No, this does not violate the HIPAA Privacy Rule. The practice should have allowed you to schedule the appointments when you indicated you were doing so at your daughter's request. Then, they should have contacted your daughter to confirm the dates/times of the appointments.

Question: *My hospital's marketing team is becoming ambitious on social media lately. They like images, of course. What should we know about posting images of patients as it relates to HIPAA?*

Answer: The HIPAA Privacy Rule considers full-face photographs to be protected health information (PHI), because they identify individuals. You should obtain written permission from patients before posting pictures of them on your social media sites.

Question: *We have recently begun to alert patients about appointments via text message. What are some things we should know about remaining HIPAA-compliant through this process?*

Answer: Because text messages could be viewed by someone other than the patient, appointment alert messages should contain the minimum amount of information necessary. Here's an example of an acceptable message:

"You have an appointment with Dr. Smith at 10 a.m. on Tuesday, August 8. Please call 999-999-9999 with questions or to cancel." The message should not contain the patient's name or any health information.

Question: *What have you seen as best practices with faxing PHI? We still rely often on faxing patient records.*

Answer: Here are some recommendations to protect faxed health information:

- Fax the minimum amount of information needed. Voluminous records should be photocopied and sent by mail or a delivery service.
- Program frequently used fax numbers into your fax machine to avoid faxing information to the wrong number.
- If the fax number is an unfamiliar one, try faxing a test document first. Call the recipient to ensure receipt of the test document before faxing PHI.
- Use a cover sheet that identifies your organization, states the legal protections for health information, and asks recipients of misdirected faxes to contact you immediately and return or destroy the information.

Editor's note: *This article originally appeared in HCPro's Revenue Cycle Advisor. Mary Brandt is a health care consultant specializing in healthcare regulatory compliance and operations improvement. She is also an advisory board member for BOH.*

CONTINUED FROM P. 1

hospital-based practices like radiology but are quickly moving into other physician specialties as well as primary care practices.

These deals are increasingly popular among physicians because the PE firms often pay more for a practice than a hospital would. PE firms also typically have more resources for capital and other improvements, such as electronic health records and infrastructure to offer value-based payment programs, says attorney Roger Cohen with Goodwin Procter in New York City. They additionally enable physicians to step back from much of the business management of the practice.

But, as with any deal, compliance issues can trip up a practice:

1. **Corporate practice of medicine prohibitions.** A lot of states prohibit non-physicians from owning a physician practice or partnering with one. This requires the practice to retain control over clinical affairs. In such states, the PE investor would buy the management company that the practice contracts with to handle business operations, and the physician corporation remains owned by the doctors, which is captive and pays a management fee to the management company. Practices can't afford to take short cuts. A physician who violates these rules can lose her license to practice medicine, warns Prives. "The physician has more to lose than the PE firm, whose liability is usually only monetary," he explains.

2. **Fraud and abuse issues.** While fraud and abuse concerns are more inherent in a deal between a physician practice and a hospital, physicians still need to comply with the fraud and abuse laws. For example, a PE firm that invests in both physician practices and ancillary providers may want to refer patients from one to the other, which could violate the anti-kickback statute, says Prives.

There's risk for the PE firm, too. The Department of Justice (DOJ) recently filed a complaint against a compounding pharmacy, Patient Care America, and the PE firm that had invested in it, claiming that they violated the False Claims Act. Including the PE firm in the complaint is a first, says Prives. The DOJ alleges, among other things, that the PE firm was actively involved in the management of the pharmacy, and that pharmacy and PE firm, needing to increase the pharmacy's profitability for a planned sale, engaged in illegal kickbacks, manipulated compounding ingredients to maximize reimbursement and participated in other unlawful activity.

3. **Date privacy and security.** HIPAA allows patient data to be shared to a potential buyer and to a management company after the acquisition as part of operations. However, a practice needs to ensure that the PE firm doesn't use the data in in violation of HIPAA or state privacy laws, says attorney Matthew Fisher with Mirick O'Connell in Worcester, Mass. For example, the practice needs to follow the minimum necessary requirement when it shares information with the firm.

4. **Other state laws.** Many states have additional statutes that can affect a PE deal. For instance, about half of states have certificate-of-need laws, which facilitate coordinated planning of new services. The laws could apply to certain types of practices, such as one with an ambulatory surgery center. Other states have banned fee-splitting with non-physicians. Any deal will need to be structured to take these restrictions into account.

5. **Past compliance problems.** A potential PE buyer will look closely at whether a practice is in compliance with applicable laws, as well as its malpractice history. A physician practice will be worth more if it has an effective compliance program, says Joseph Tomaino, CEO of Grassi Healthcare Advisors in New York City. "Physicians also need to clean up their books and not run personal expenses through the practice," he says.

RESOURCE:

- False Claims Act complaint against Patient Care America and its PE firm: *www.justice.gov/opa/pr/united-states-files-false-claims-act-complaint-against-compounding-pharmacy-private-equity*

News briefs

Little white lie leads to an orange jumpsuit for Florida doctor. You know that doctors shouldn't lie to auditors about their health care claims. A prosecutor can use a fib to show that improper claims constitute fraud. But alternative facts that aren't even related to claims can constitute obstruction, and result in jail time. John Janick, M.D., of Port Charlotte, Fla., was sentenced to 5 months in prison and 3 years of supervised release for obstructing a Medicare audit. In addition, the doctor will have to pay Medicare $118,831 in restitution, the Department of Justice (DOJ) announced in a Sept. 14 press release:

"According to the plea agreement, Janick lied to a Medicare program integrity contractor who was auditing Janick Medical Group. Specifically, Janick falsely claimed that a third-party employer was paying rent for office space utilized by his wife, Lisa McLaren Janick. The office space, located within the Janick Medical Group practice, was used by Lisa McLaren Janick to improperly access sensitive patient data that was then used to generate referrals from Dr. Janick to her third-party employer without regard for medical necessity."

It isn't clear whether the audit was related to McLaren Janick's activities, the practice's claims or a combination of the two. But Janick may be the lucky one in this case. Lisa McLaren Janick pleaded guilty to two counts of health care fraud, according to a DOJ press release published July 20. She could receive up to 20 years in federal prison for each count. The press release for Janick's sentencing is available here *www.justice.gov/usao-mdfl/pr/port-charlotte-doctor-sentenced-five-months-prison-obstruction-audit*. Read about McLaren Janick's guilty plea here *www.justice.gov/usao-mdfl/pr/port-charlotte-woman-pleads-guilty-health-care-fraud*.

False billing scheme stretched from the East Coast to Egypt. Moustafa Aboshady, M.D., has been convicted for his role in a pain practice's plot to defraud Medicare and private insurance companies, the Department of Justice announced Sept 21. Aboshady worked for a pain management chain with locations in Rhode Island and Massachusetts. The conspiracy involved a number of doctors, including the practice's owner falsifying medical records for patient visits and records for urine drug tests. Employees at a satellite office in Cairo were instructed to create false electronic signatures and time stamps to help perpetrate the fraud.

"The charges provide for a sentence of no greater than five years in prison, three years of supervised release, a fine of $250,000 and restitution. Sentences are imposed by a federal district court judge based upon the U.S. Sentencing Guidelines and other statutory factors," the press release states. To read the press release, go to *www.justice.gov/usao-ma/pr/physician-convicted-false-billing-scheme*.

Subscriber information

EDITORIAL
Have questions on a story?
Call toll-free: **1-855-CALL-DH1**

Content Manager, Medical Practices:
Karen Long, x6016
klong@decisionhealth.com

Editor:
Marla Durben Hirsch, x6015,
mdurbenhirsch@decisionhealth.com

Julia Kyles, CPC, x6015,
jkyles@decision health.com

Join our DecisionHealth — Medical Practice & Hospital community!
www.facebook.com/DecisionHealthMP
www.twitter.com/DH_MedPractice
www.linkedin.com/groups/4048762

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

REVENUE CYCLE FORUM
To join the free medical practice revenue cycle forum, our free Internet forum for revenue cycle specialists, including compliance managers and auditors, go to *http://practiceforum.decisionhealth.com/* and register.

Medical Practice Compliance Alert® is a registered trademark of DecisionHealth. *Medical Practice Compliance Alert* is published 12 times/year by DecisionHealth, 100 Winners Circle, Suite 300, Brentwood, TN 37027. ISSN 1047-1863. *www.decisionhealth.com* Price: $547/year.

CONTINUED FROM P. 1

Protect PHI when it moves to and from business associates

BY **MARLA DURBEN HIRSCH**

The recent settlement agreement between the HHS Office for Civil Rights (OCR) and the now-shuttered medical records storage company FileFax Inc. is a good reminder that providers and business associates need to comply with HIPAA and protect PHI not only when they possess or store it but also when they transmit it to each other (*MPCA 8/18*).

HIPAA allows covered entities to disclose PHI to their business associates but doesn't specify how to share it.

One of the most common ways to share data is electronically, says attorney Elizabeth Litten with Fox Rothschild in Princeton, N.J. When maintaining, storing or transmitting electronic PHI (ePHI), the parties need to comply with the HIPAA security rule's technical, physical and administrative safeguards to ensure the data's confidentiality, integrity and security. For example, the practice must have policies and procedures regarding how PHI will be protected while the data is in motion, maintain a log of file transfers and a mechanism to control who has access to the data (*MPCA 4/17*).

The safest way to transmit ePHI is through a closed network. HIPAA also allows providers and business associates to network their computers to share data so long as they have evaluated the risks associated with networking, such as firewalls, and meet the security rule's safeguards.

Take precautions with open networks

However, because covered entities and their business associates often are not connected via a direct network, they generally transmit ePHI via an open network, such as email. HIPAA's security rule allows transmittal via an open network, but the rule still requires that the PHI be adequately protected and the parties comply with the security rule's safeguards.

For transmission security in an open network, that also means that the covered entity needs to consider "integrity controls" (i.e., that the data sent is the same as the data received) as well as encryption. If your practice's policies call for the use of encryption, make sure that everyone follows the protocol.

The OCR's recent imposition penalty on the University of Texas' MD Anderson Cancer highlights the importance of following through with encryption policies. The OCR fined the center $4.3 million for several large-scale breaches that occurred because the center didn't follow its written encryption policy (*MPCA 6/18*).

To use encryption, the covered entity needs to determine whether the business associate can accept the encrypted emails, says Litten. If not, then the parties will need to send the ePHI through a third-party secure messaging application and use secure methods to retrieve it, such as use of a password.

Paper records need protection too

A lot of PHI is still in paper form. If the covered entity or business associate is transmitting hard copy PHI, make sure that the PHI is being sent in a sealed format and that someone has to sign for it, says attorney Michael Kline, also with Fox Rothschild.

And that fax machine? Because it's very hard to ensure that the PHI will be protected, where it's being received and because the machine will likely retain the PHI in its own memory, causing additional risk, don't use this method, suggests Litten (*MPCA 1/18, 12/17*). "You're better off using scan and email," she says.

RESOURCES:

- FAQ use of email for sending PHI: *www.hhs.gov/hipaa/for-professionals/faq/2006/does-the-security-rule-allow-for-sending-electronic-phi-in-an-email/index.html*
- Decision against MD Anderson Cancer Center: *www.hhs.gov/about/news/2018/06/18/judge-rules-in-favor-of-ocr-and-requires-texas-cancer-center-to-pay-4.3-million-in-penalties-for-hipaa-violations.html*
- FAQ on networking computers: *www.hhs.gov/hipaa/for-professionals/faq/2017/does-the-security-rule-allow-you-to-network-computers/index.html*

OIG, CMS or DOJ? Look at options before making self-disclosure

BY **ROY EDROSO**

If you've detected a pattern of overpayment or other malfeasances at your practice that could bring the attention of the feds, in addition to repaying or correcting the issue, you should self-disclose — but first choose carefully among the agencies that offer this option.

The HHS Office of Inspector General (OIG) issues reports of self-disclosure settlements with providers who discovered issues in their billing or hiring and thought it wise to get in front of those issues before being hunted down by legal or regulatory authorities and fined, penalized or, in some cases, even imprisoned. Recent OIG settlements have seen providers owning up to hiring excluded providers, possibly violating self-referral laws by awarding "leases that were below fair market value" to other providers, providing services without the "requisite level of physician supervision" and filing claims without "sufficient documentation to justify the assigned code level." Settlements range from the tens of thousands to the tens of millions of dollars.

But OIG's not the only recourse for providers in a jam: If you have Medicaid issues, for example, your state will have a local Medicaid inspector general's office to approach, says Stephanie Fiedler, director of revenue advisory services for Grassi Healthcare Advisors in New York City. Providers with Medicare issues can under certain circumstances skip OIG and go to the Department of Justice (DOJ) via their local U.S. attorney's office or to CMS via their Self-Referral Disclosure Protocol, established by the Affordable Care Act, notes Timothy B. Adelman, attorney with Hall, Render, Killian, Heath & Lyman in Annapolis, Md.

OIG self-disclosures are typically "for False Claims Act violations that come with penalties," says Adelman, and overpayments can easily become FCA cases under recent regulation. CMS disclosures "are typically for Stark violations," but may also include failures to comply with certain conditions of payment or participation — for example, the *bona fide* employment relationship exception. Self-disclosure to the DOJ can be for either kind of issue, says Adelman.

Your consideration of whom to approach will be colored by whether you anticipate fraud charges when the issue is revealed. "CMS does not have authority to waive prosecution under False Claims [Act]," says Adelman. "They typically coordinate with DOJ and/or OIG, so if there is the appearance of fraud, it will wind up in the hands of the other guys."

On the other hand, "if there's no fraud, OIG and DOJ don't care," Adelman says. Say you have a largely technical issue — for example, an improperly signed contract, which technically violates Stark but may otherwise be compliant in terms of fair market value and other Stark requirements. "You could sell it to CMS, and typically you'll get a more favorable settlement" than DOJ or OIG would give, says Adelman.

But let's say you paid someone above market value for services, which infers paying for referral and would be fraud. Then, says Adelman, you might want to go to DOJ or OIG. At DOJ, you may even get a break: Some local U.S. attorneys have been known to mark down penalties substantially. But the trend of late has been for the

U.S. attorneys to "kick it to main Justice [in Washington, D.C.]," which has more rigid processes in terms of calculating the damages, says Adelman.

How much to disclose?

Because the whole idea of self-disclosure is to avoid or reduce penalties that might appertain if the feds find out about your issue, the simplest standard is to report anything for which you could be penalized. But what about overpayments? OIG's minimum settlement amount for self-disclosure is $10,000, but does that mean that if you find a couple of overcoded claims that add up to that amount, you should enter its self-disclosure protocols?

You are definitely obliged by regulation to look for overpayment patterns when you discover any overpayments at all. "After finding a single overpaid claim, we believe it is appropriate to inquire further to determine whether there are more overpayments on the same issue before reporting and returning the single overpaid claim," says CMS in its 2016 final rule on the Reporting and Returning of Overpayments. The provider is instructed to "use a probe sample and then incorporate that probe sample into a larger full sample as the basis for determining an extrapolated overpayment amount."

Once you extrapolate the amount, you can just pay it back to the contractor — or you can also self-disclose. The decision to self-disclose, says Fiedler, "depends on the volume and duration of the issue. If the issue is pervasive throughout the system or was identified to have happened over a long period of time, it could warrant a self-disclosure."

For example, "if you find [in an audit] that 90% of provider's services are overbilled, I would expand the audit and take further steps." Also: "Has it been three months or five years? ... If I found that all or most of a particular type of procedure was billed incorrectly, I would then move toward trying to isolate when it began, volume, one provider or everything, etc., to quantify the issue."

But there's no hard and fast rule, says Fiedler, so use common sense: "[A small amount] in a $200 million business distributed over multiple payers may not be something that warrants a self-disclosure," she says. "Each situation needs to be evaluated on its own merits."

RESOURCES:

- Reporting and Returning of Overpayments final rule: *www.gpo.gov/fdsys/pkg/FR-2016-02-12/html/2016-02789.htm*
- OIG self-disclosure reports: *https://oig.hhs.gov/fraud/enforcement/cmp/psds.asp*
- OIG self-disclosure protocol: *https://oig.hhs.gov/compliance/self-disclosure-info/files/Provider-Self-Disclosure-Protocol.pdf*
- CMS voluntary self-referral disclosure protocol: *www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral/Downloads/FAQs-CMS-Voluntary-Self-Referral-Disclosure-Protocol.pdf*

Penalties appertaining to health care

Stark Law violations

- Overpayment/refund obligation
- False Claims Act (FCA) liability
- Civil monetary penalties ($24,253 per claim) and exclusion for knowing violations
- Civil assessment of up to three times amount claimed

FCA liability

- Three times single damages (claims at issue) plus $10,957 to $21,916 per false claim submitted

Anti-kickback statute violations

Criminal penalties

- Criminal fines up to $100,000
- Up to 10 years in prison

Civil/administrative penalties

- FCA liability
- $74,792 civil monetary penalties per violation
- Civil assessment of up to three times amount of kickback
- Potential exclusion

Unlisted codes a poor bet for success, especially if doctors miss a memo

BY **ROY EDROSO AND JULIA KYLES, CPC**

Providers don't like to use unlisted codes if they can help it, and no wonder — the denial rates are ridiculous.

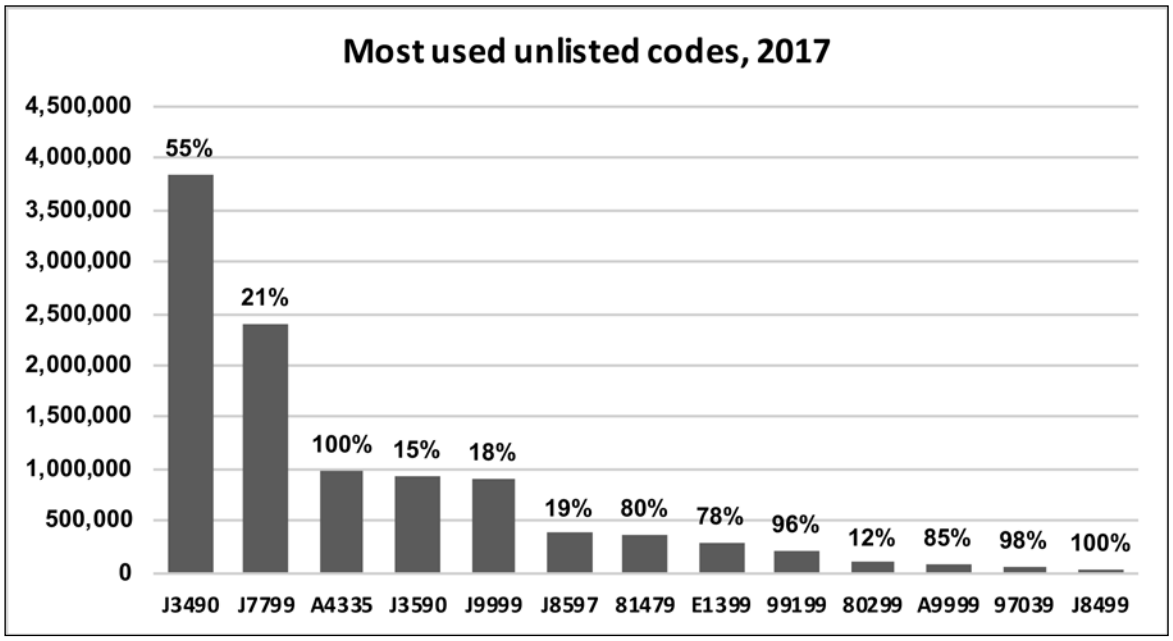
Unlisted codes are meant to be used for products and procedures that are not described by a specific CPT code or HCPCS code. Providers must make sure that they use unlisted codes as a last resort, and that includes checking the Category III CPT codes to make sure the service isn't listed there. Medicare and private carriers rarely cover Category III codes, which may tempt practices to report an unlisted code for the service. However, that would be improper coding and could lead to accusations of fraud.

In addition, unlisted codes mean more work for the provider. The clinician will need to include documentation that details what she did with the claim.

CMS has in the past sometimes directed providers to use unlisted codes as placeholders for new services — for example, when they first started paying for tobacco-cessation counseling absent any tobacco-related illness. More commonly, CMS will authorize payable codes to end the use of unlisted codes, as in the proposed 2019 Medicare physician fee schedule, which promises a new code for biopsy or excision of inguinofemoral nodes and asks providers to use that instead of the customary unlisted codes they'd been using.

But unlisted codes rarely work out well for most providers. The 166 unlisted codes claimed by Medicare providers in 2017 had an aggregate denial rate of 55%. And 19 of the codes had 100% denial rates, and 18 had rates between 90% and 99%. As indicated in the chart, of the 13 unlisted codes that were claimed most often in 2017 — comprising 10.6 million of the 17.4 million total unlisted code claims that year — eight had a denial rate of more than 50%.

Unnoted policy changes may make some unlisted code denial rates worse; for example, in 2015, CMS instituted the use of **Q9977** (Compounded drug, not otherwise classified) for all unclassified compound drugs, which many providers had been claiming with **J3490** (Unclassified drugs). Continued inattention to that change may have something to do with J3490's 55% denial rate. Check the website of your Medicare administrative contractor as it generally has thorough guidance for claiming unlisted codes.



Source: Part B utilization data

How did you get this email?

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 Brad Forrister at 1-800-727-5257 x8041 or email him at *bforrister@blr.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.