G2 INTELLIGENCE
A DIVISION OF PLAIN LANGUAGE MEDIA

G2 Compliance Advisor

For Clinical and AP Laboratories and Pathology Practices

April 2015

Inside this issue

www.G2Intelligence.com

Note from the Editorial Director

Christopher Young, editor of *G2 Compliance Advisor*, is retiring this month. The G2 family would like to thank Chris for his invaluable contributions, not only in his role as a G2 editor in recent years but as a source quoted in articles and as a presenter at numerous G2 live events over nearly two decades. Chris has also served the laboratory industry for more than 40 years, working directly in the laboratory and providing guidance since 1997 as a compliance professional and owner of Laboratory Management Support Services. We wish him all the best in his retirement. Chris may be retiring as Editor of *G2 Compliance Advisor* but he has agreed to periodically contribute to the G2 family of publications.

Upcoming G2 Events

Lab Institute
October 14-16, 2015
Hyatt Regency Washington DC on Capitol Hill
www.labinstitute.com

HDL, Singulex Agree to Settle AKS, FCA Charges for $48.5 Million

Labs should revisit their arrangements with referring physicians now that lab giant Health Diagnostic Laboratory, Inc. (HDL) and Alameda, Calif., based Singulex, Inc. have agreed to pay $47 million and $1.5 million respectively to settle claims of paying kickbacks and conducting medically unnecessary testing.

Under the deal, announced by the U.S. Department of Justice (DOJ) April 9, HDL and Singulex will settle allegations that they induced physicians to refer to them for blood testing by paying them processing and handling fees of between $10 to $17 per referral and routinely waived copayments and deductibles, causing the submission of false claims to federal health care programs. Both companies will also enter into corporate integrity agreements with the government, according to the DOJ's press release.

The two settlements stem from three lawsuits filed by whistleblowers under the False Claims Act. The whistleblowers can receive up to 25 percent of the settlement proceeds; the DOJ has not released the exact amounts that they'll receive under these settlements.

Continued on page 9

Cyber Criminals Want Your Data: Protect Your Patients—and Your Lab

Recent data breaches, from the much-publicized hacks of Sony and the retailer Target, to those more close to home: Anthem and Premera Blue Cross, two of the nation's biggest health care insurers, have spotlighted the risk of cyber attack. The risk is so great that this February President Obama held a cyber security summit to discuss measures to address both public- and private-sector threats. Last spring, the FBI released a private industry notification (PIN) to the health care industry stating that health care is particularly vulnerable to cyber attack. PINs aren't made public, but according to a report by Reuters, which obtained a copy of this one, it reads in part, "The healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely."

Continued on page 2

Cyber Criminals Want Your Data: Protect Your Patients—and Your Lab, *from page 1*

Cyber attacks are also likely because health care data is particularly coveted by those who trade in black-market data. According to Alan Paller, director of research for the SANS Institute, an organization that offers IT security training and certification, "People pay as much as 20 times as much for health care data as they do for credit-card data." It's not hard to see why. With credit card data, a black-market purchaser gets names, addresses, social security numbers. Health care records provide much more information, including next of kin, whom to call in case of emergency, and of course, details of health conditions. Health care data can also provide information useful in obtaining prescriptions for drugs. In addition, credit card data has a limited usefulness—people cancel their cards and change their account numbers when they've been hacked—but health care data is permanently useful. You aren't going to change your family members or the fact that you have type 2 diabetes when your health care records are stolen.

If your lab is the victim of a cyber attack, or your data is compromised in any way (even an internal mistake, such as a lost laptop or flash drive), you are required to file a report with the Office for Civil Rights and notify anyone whose data may have been compromised.

—Rick Hindmand, Health Care Attorney

It's likely that the problem is already worse than most people realize, says Paller. Not all cyber attacks, perhaps only a small percentage, make the news. Cyber extortion may be as common as cyber theft. A hospital or other health care entity may receive an email telling them that their data has been stolen, providing evidence of the theft, and demanding a ransom to keep the theft from being publicized. Even if the victim pays the ransom (and the FBI typically advises them to do so, says Paller) the data is still sold—it's a win-win for the thieves—but the public is none the wiser. Because of the delicate nature of investigations into this type of crime, and the fact that a system is particularly vulnerable to subsequent attacks until there has been time to locate the breach and repair the defenses, the authorities often recommend delaying a public statement, says Lisa Clark, health care attorney with Duane Morris in Philadelphia.

Big Trouble

If your lab is the victim of a cyber attack, or your data is compromised in any way (even an internal mistake, such as a lost laptop or flash drive), you are required to file a report with the Office for Civil Rights (OCR) and notify anyone whose data may have been compromised, explains Rick Hindmand, a health care attorney with McDonald Hopkins in Chicago. If more than 500 individuals are involved, the breach must be made public as well. "The report filed with the OCR may generate an investigation, and depending on the circumstances, could result in penalties," says Hindmand. In addition, the Federal Trade Commission can take enforcement action for inadequate information security practices as "unfair acts and practices" under section five of the FTC Act, adds Paula Stannard, an attorney specializing in health care law at Alston and Bird, and former deputy general counsel and acting general counsel of the U.S. Department of Health and Human Services.

However, penalties are likely to be the least of your problems if you've had a serious data breach. Though HIPAA rules do not allow for a private cause of action, there are several ways for victims to file individual suits. "A number of courts, especially state courts, have looked to HIPAA as establishing a standard of care for health privacy in negligence actions," explains Stannard. "If you fail to meet that standard of care,

G2 Compliance Corner

One of the tougher issues a non-lawyer compliance officer faces, is a challenge to their decisions and recommendations by other members of the management team. This happens more often when the person is new to the company or the position. In a large proportion of these challenges, the challenger cites a lawyer's comments or an interpretation they saw in a newsletter or on the Internet, or something they believe a competitor is doing. In the worst of all cases, the challenger is the chief executive. The laws and regulations governing health care change often and can have unique interpretations when applied to clinical laboratories. A person unfamiliar with these differences can misinterpret something that is intended for a different sector of health care. Additionally, most compliance decisions, particularly in the area of anti-kickback and Stark, are based on the facts and circumstances unique to a particular situation.

If the compliance officer does not effectively deal with these challenges, it can undermine their authority and make their job harder or even impossible. Here are some recommendations that will help you avoid or deal with this should it happen to you:

- Establish good working relationships with other members of the management team. Let them know you are there to *support* what is best for the laboratory, not only from a legal and regulatory perspective but also from a business perspective.
- Never automatically assume that you are right and they are wrong.
- If you don't already know, ask for the source of their information so you can research it. Even if you think you know, ask anyway in case they are looking at something else and misinterpreting it.
- State the reasons for your decision clearly and concisely and provide documentation to support them.
- Create a library of questions and cases that come up, your response and the documentation you provided at the time. Many times the same or similar questions will come up again and again. Consistency in your responses is an important aspect of establishing credibility. If your answer is going to be different make sure you include the reason it is different.

Credibility and trust are two of the compliance officer's most important traits. Trust and credibility have to be earned, they are not just assumed because you have the title. A track record of good decisions based on thoroughly researched and documented responses will go a long way toward establishing those traits with your management team.

plaintiffs may have a private cause of action based on state negligence law in state or federal court."

If your security is breached, you'll encounter many other, often unexpected expenses, even if the OCR doesn't impose penalties and no patients file suit. The costs include legal representation, forensics to determine the cause of the breach and make repairs, notifying patients whose data was compromised, setting up a call center to answer patient questions, credit monitoring, and identity-theft protection for affected individuals—all this can add up very quickly. A 2014 study by Ponemon Institute estimated the cost of a data breach to be around $200 per record in the United States, with the health care industry having one of the highest costs per record of all industries.

How to Protect Your Data—And Yourself

So what can you do besides wait and hope you're not one of the ones who gets hit? You've had a risk analysis, your staff has been through HIPAA training, you've bought the latest software and keep up with security upgrades. What more can you do?

"If you do everything right and meet HIPAA's 'reasonable standards' of training, risk analysis, and so on, and you still get hacked, you aren't likely to face any penalties, and your chances will be better in court if you are sued. But you should keep in mind that doing the minimum to satisfy the HIPAA rules might not be all that you can do," says Hindmand. If you want to take security protection seriously—and it is in your interest as well as that of your patients to do so—then you may need to up your security game. Paller offers a few tactics you may not have thought about:

- Take special precautions with all access points, places where physicians, patients, clinics, or other labs can access your data. If physician clients have passwords that allow them to access your data, they

If the good news is that there is a probably a lot more that you can do to protect yourself and your patients' data, the bad news is that even the very best you can do will probably not be enough in the long run.

may not keep it secure. Use the latest encryption methods for an additional level of protection. Make sure all email communications with providers are encrypted. There are many potential access points to your data. These access points may seem harmless in the big picture of protecting patient privacy, but are potential weak spots that can be exploited by hackers.

- Periodically update your security risk analysis. Don't do just the basic minimally required analysis, hire security consultants and dig deep.
- Encryption is the expectation—passwords are not enough. Encrypt all sensitive data.
- Move to next generation firewalls. These protect against sophisticated attacks by identifying what kind of data is coming through the firewall and making a determination about how to respond based on the type of traffic coming through the network. These newer firewalls are far superior to the previous generation.
- Consider installing end-point protection that tests attachments by opening them in an enclosed space (called a sandbox). This could be especially useful when getting patient data from hospitals and clinics.
- Perhaps most important of all is white listing. This keeps people—even if they can get in to your system—from being able to install any applications on your computer. People often don't take this relatively simple step because it can be inconvenient, says Paller. If an employee is working from home and needs, say, to connect to a printer, if he hasn't been added to the white list, he won't be able to get the job done until he's back in the office. This inconvenience is small compared to the protection offered by white listing.
- Consider buying cyber security insurance to cover the costs you will encounter in case of a breach—even if you are cleared of wrongdoing.

These measures may cost time, money and other resources, but you'd be wise to at least consider going a few steps beyond the basic security measures. The threat is real, and as a member of the health care industry, you are a juicy target for some of the most sophisticated cyber criminals out there.

If the good news is that there is a probably a lot more that you can do to protect yourself and your patients' data, the bad news is that even the very best you can do will probably not be enough in the long run. The world of cyber security "is an arms race," says Paller. It is a constant struggle to stay one step ahead of cyber criminals.

But if it's an arms race, it's also an odds game. By going beyond the basics, you definitely reduce the chances that you'll be hit, and, says Hindmand, the more precautions you've taken the less it will cost you if you are hit.

Takeaway: Cyber attacks are a very real threat, and your responsibility to protect patient data goes well beyond HIPAA training and risk analysis. But actually protecting that data may be a greater challenge than you realize. G2

COMPLIANCE PERSPECTIVES

OIG Advisory Opinion Makes Convenience and Efficiency Suspect

Exclusive payer contracts create challenges and hassles for laboratories outside the contract and physicians who do business with those laboratories. A recent Advisory Opinion from the U.S. Department of Health and Human Services' Office of Inspector General (OIG) addresses free laboratory services and pull-through strategies that developed in response to exclusive contracts. The OIG's opinion finds potential anti-kickback violations in efforts intended to increase efficiencies in health care delivery. Laboratory compliance officers need to understand what the OIG's Advisory Opinion could potentially mean for waiver arrangements.

The Proposed Arrangement

The laboratory requesting the opinion described a proposed arrangement with physicians that would waive laboratory charges for patients insured under an exclusive contract that named another laboratory as the only covered laboratory. That plan allowed the laboratory to service all the physician's patients, making health care delivery more efficient within the physician practice. The arrangement was motivated by physician preference for dealing with one laboratory for consistent test result reporting (avoiding use of different reference ranges) and "ease of communication"—using one interface for electronically transmitting orders and receiving results, rather than multiple interfaces required when dealing with more than one laboratory.

Physicians would need to attest that neither the physicians or the practice were receiving any financial benefit from the provision of free laboratory services to their patients—including any benefit (or penalty) derived from an incentive plan addressing laboratory utilization. The only item or service or benefit provided from the laboratory to the physician would be the limited-use interface allowing the physician to communicate with the requesting laboratory. The laboratory mentioned that some vendors charged its physician practice clients monthly maintenance fees for the interface and the laboratory wouldn't pay those fees on behalf of the physicians.

The OIG concluded the arrangement "would offer physician practices a means to work solely with the Requestor, reducing administrative and possibly financial burdens associated with using multiple laboratories."

Potential violations

The OIG found this arrangement could violate the anti-kickback statute, which prohibits payment of any remuneration for a referral or recommendation for a service reimbursed by federal health care programs. Violation of that law depends on the parties' intent (knowing or willful conduct is required) but even if just one purpose for the arrangement is to induce or reward referrals, it can be a violation. The penalties for violations include fines (up to $25,000), imprisonment and exclusion from participating in federal programs. Note that submission of a Medicare claim for payment that resulted from an illegal kickback can also result in penalties under the False Claims Act.

Although it conceded that provision of limited use interfaces to the physicians was not remuneration, the OIG was concerned referring physicians received remuneration via the

combination of the "convenience of receiving all test results with consistent reference ranges" and the ability to avoid multiple interface maintenance fees that would be paid by the physician practices. The OIG concluded the arrangement "would offer physician practices a means to work solely with the Requestor, reducing administrative and possibly financial burdens associated with using multiple laboratories." Therefore, the OIG couldn't "rule out with sufficient confidence the possibility that" remuneration was being offered to induce or reward referrals.

The OIG was also concerned that the laboratory would be charging Medicare and Medicaid "substantially more than their usual charges to other payors for the same items or services," which is grounds for permissive exclusion. The OIG appears to have interpreted the substantially in excess rule in the past to mean that if 50% (or more) of the laboratory's charges (excluding Medicare and Medicaid charges) are less than what is being charged Medicare, that lower rate being charged may be considered the laboratory's usual charge. Thus, if half of the laboratory's charges were waived as described in this proposed arrangement, "the laboratory's usual charge might be considered zero by the OIG," explains Maryland health care attorney Robert E. Mazer of Ober Kaler.

In this case, the OIG was concerned that close to or more than half of non-federal health care program business was being provided for free because the data submitted indicated 70% of physician clients of the laboratory had patients subject to exclusive contracts and within those physician practices, between 10% and 40% of the patients had exclusive contracts. These numbers caused the OIG to be concerned: "with percentages that high, it is plausible that more than half of the non-Medicare or non-Medicaid patients would be receiving free services, while Medicare and Medicaid would be charged at the regular rate." This gave rise to a two-tiered pricing structure with "substantial number of patients" getting free services "regardless of financial need."

Why the Opinion is Significant

The OIG's concern about waiving fees is nothing new. Mazer notes the OIG specifically addressed the issue of such waivers in a 1994 Fraud Alert, yet it doesn't reference that Alert in the Advisory Opinion. The opinion has caused concern within the industry because of the facts the OIG relied on in finding potential improper remuneration.

Mazer highlights the two facts that the OIG found in combination amount to remuneration:

1. "it is more convenient, more efficient, for the physician practice to use one laboratory" and
2. "elimination of interface maintenance fees that would be paid by the physician practices."

"The first fact may be present in almost all instances," he says. If the OIG is saying remuneration has been provided when an arrangement "makes it administratively more convenient or efficient," notes Mazer, that reasoning conflicts with goals of increasing efficiency and cost savings in the health care delivery system. He adds, "Convenience is a slippery slope." "It's hard to analyze that." Additionally, Mazer expresses surprise at

the OIG's reliance on the interface maintenance fee "particularly because it is probably so infrequently the case that the physicians actually pay for it." He explains, "the OIG effectively treats the elimination of unnecessary maintenance fees as if the laboratory offering the program had actually paid the maintenance fee for which the physician otherwise would have been responsible."

The opinion and the lack of clarity about when convenience and efficiency cross the line into improper remuneration could stifle efforts to streamline health care delivery. "It is certainly possible that some laboratories will terminate these types of arrangements based on the advisory opinion," observes Mazer.

"The advisory opinion could have implications beyond arrangements for free testing. Laboratories could be concerned that it ushers in a new era of anti-kickback statute enforcement under which any arrangement that provides a referral source with 'convenience' or increased 'efficiency' might result in potentially prohibited 'remuneration,'" he explains. "Any such policy would appear counterproductive to efforts to increase efficiency of health care services."

But laboratories are not without recourse in addressing this opinion. Mazer advises, "There is nothing to prevent a laboratory from submitting its own request for an advisory opinion, perhaps with more favorable facts, such as assuring the OIG that the arrangement would not be offered when the medical practice was paying interface maintenance fees." The OIG has also previously provided written clarification of advisory opinions, such as the letter referred to by the OIG in the advisory opinion regarding the substantially in excess provision.

5 Tips for Avoiding Kickback Liability When Waiving Charges

With regard to kickback liability, while Mazer isn't sure if the OIG would "actively pursue these types of cases, particularly if the physician practice isn't paying the interface maintenance cost," he cautions that this advisory opinion could "pique the interest of qui tam relators." Additionally, as to excessive charges, Mazer says to his knowledge "the OIG has never pursued a case based solely on the substantially in excess provision." But it may not be prudent to ignore this provision. "You still have to do your due diligence," warns Mazer and examine your charges to determine if there is any potential violation.

With that advice in mind, we've compiled five tips to help your lab avoid liability for kickbacks or excessive charges due to waiver of fees.

#1 Audit your waived charges policies and agreements. As Mazer suggests, do your due diligence. Take this opportunity to review any policies, procedures and agreements that address reduced payment amounts, including waiver of charges. Look for violations of the anti-kickback statute and the substantially in excess provision.

#2 Determine usual charges. You will need to calculate how waived charges affect determination of your "usual charge." As Mazer advises, even though the OIG hasn't actively pursued cases against providers under the substantially in excess provision, you still need to do your due diligence and review charges to make sure you aren't in violation. Document the findings of this charge review so you can hopefully dispel OIG concerns if such an issue should ever arise.

COMPLIANCE PERSPECTIVES

Unfortunately, as even the OIG conceded in the opinion, there is not a lot of guidance on how to determine your usual charge and compare it to Medicare charges.

"A first step may be to compute the volume of tests that have been provided without charge and compare that number to the total volume of tests billed to payors other than Medicare and Medicaid," suggests Mazer. "As the OIG indicated, if the percentage of free tests is substantially below 50%, then the arrangement should not cause concern under this statutory provision."

"The difficult issue is whether there are other discounted charges that need to be part of the calculation," he says. "The OIG stated that the substantially in excess provision was not intended to prevent negotiated payment arrangements with private insurers, however, it has not unequivocally stated that such charges can be excluded from the calculation of a hospital's usual charge."

#3 Look for benefits/remuneration to referral sources. Consider what benefits to referral sources, financial or otherwise, may result from the waiver policy or arrangement. As Mazer explained, the OIG addressed waiver of charges to private plan members in its 1994 Special Fraud Alert and indicated such waivers were permissible as long as the physician practice wasn't benefitting financially, such as through incentive plans and utilization programs. The advisory opinion indicates that additional types of benefits could potentially be considered remuneration.

This is where it gets tricky because the OIG didn't provide significant explanation of the avoidance of administrative burdens and at what threshold efficiency becomes remuneration.

#4 Make sure physicians aren't getting reimbursed for anything related to the laboratory services. In the Advisory Opinion, the requesting lab was only offering the proposed arrangement to physician clients who sent their patients to the laboratory's draw stations. The physicians were not drawing the samples themselves. In fact, in a footnote, the OIG noted that the laboratory did have some physician clients who drew the patients' blood and the laboratory wouldn't offer the proposed arrangement to those physician clients. This factor is important because if the physicians were drawing the blood samples, then the physician could be getting reimbursed for that service. That could be considered a financial benefit to the physician. So, make sure if you are going to develop a waiver program that no part of the service is reimbursable directly to the physician.

#5 Get physician attestation of no benefit. Mazer suggests that laboratories with arrangements involving free services require physicians "sign an attestation that they don't receive any financial benefit from the free testing, including the elimination of any monthly interface fee." The arrangement in this case required similar attestations from physicians that they didn't receive any benefit but didn't mention such interface fees. So your attestation should include reference to such fees, including the utilization incentives mentioned in the 1994 Fraud Alert as well as a general catchall disclaiming any other financial benefit. But remember, just getting that attestation isn't a defense if in reality referring physicians are receiving some financial benefit.

Source: U.S. Department of Health and Human Services, Office of Inspector General, Advisory Opinion 15-04 (March 18, 2015).

HDL, Singulex Agree to Settle AKS, FCA Charges for $48.5 Million, *from page 1*

The government has also joined—or "intervened"—in whistleblower lawsuits against Berkeley HeartLab, Inc., BlueWave Healthcare Consultants, Inc. (the apparent middleman in the arrangement between HDL and the physicians), and former HDL CEO Tonya Mallory.

HDL issued its own statement regarding the settlement, indicating that it was "pleased" with it and stressing that it was part of an industry-wide investigation into the diagnostic lab industry, not one merely targeting HDL:

> In June 2014, when the government for the first time issued new guidance stating that the payments presented risk, HDL, Inc. immediately stopped paying processing and handling fees to referring providers. HDL, Inc.'s comprehensive biomarkers provide a far broader and deeper picture of patient health than the traditional reactive model based on technology available decades ago, and aid physicians in identifying risks, setting appropriate therapeutic targets and delivering the right treatments at the earliest meaningful time. Each physician chooses the testing he or she would like to perform in the best interest of his or her patients, and HDL, Inc. is proud to continue to partner with physicians to offer this critically important testing service.
>
> We have taken the step of resolving this matter in order to put these allegations, which stemmed from historical practices once common in the industry, behind us. These allegations were made against a number of companies operating in the clinical laboratory industry by individuals who stand to personally profit by making these allegations.
>
> Reaching this agreement enables HDL, Inc. to avoid the distraction of what could have been years of uncertainty associated with protracted and expensive litigation. The settlement allows us to move ahead with our important work of helping improve the health of millions of Americans.

HDL also reiterated that it will not be excluded from participation in the Medicare and Medicaid programs and that the settlement "does not mean that HDL, Inc. engaged in any wrongdoing" and "is not an indication that any conduct was improper or unlawful."

The deal did not come as a surprise; the *Wall Street Journal* (*WSJ*) had leaked news of it in March. *WSJ* had also reported in 2014 that HDL had been paying physicians for blood sample referrals and some referring physicians had received thousands of dollars from the company a week.

HDL, clearly displeased that the *WSJ* had leaked news of the impending settlement before it was finalized and formally announced, issued its own statement in March specifically denying wrongdoing and asserting that it has "consistently sought to comply with all applicable legal and regulatory requirements, and [is] committed to continuing to do so."

"We wish to make it clear that HDL, Inc. has worked cooperatively with the Department of Justice since the inception of its investigation of various diagnostic laboratory industry practices, many of them common within the industry," HDL stated.

This settlement does not end HDL's other legal troubles. As we have reported in the December 2014 and January 2015 issues of *G2 Compliance Advisor*, HDL is still embroiled in a lawsuit brought by Cigna alleging that it unlawfully waived copayments and coinsurance, as well as defending itself in a breach of contract action by BlueWave. HDL terminated its contract with the consulting company after the Department of Health and Human Services' Office of Inspector General issued its special fraud alert in 2014 against these lab-physician payment agreements.

For some advice about how to avoid similar legal issues relating to relationships with referring physicians, see the next story below.

Takeaway: In the wake of last year's fraud alert about payments to referral sources, the HDL and Singulex settlements could be the first of several agreements concerning such payments. G2

Recent Enforcement Calls for Scrutiny of Arrangements With Referral Sources

The U.S. Department of Health & Human Services' Office of Inspector General (OIG) has long found laboratory deals with physicians to be inherently suspect. Recent enforcement efforts and settlements highlight the compliance risks created by arrangements between laboratories and referral sources. Last year's fraud alert regarding payments to referring physicians and the recent HDL and Singulex settlements (see story on page 1) are significant because they send a strong message that labs are a front burner concern for the government, and that they will be subject to increased scrutiny. The OIG has also previously blasted a no-risk lab agreement that would have allowed physician practices to enhance their revenue, in its Advisory Opinion 13-03; prosecuted labs and physicians for unlawful involvement in kickback schemes with labs; and nixed a proposed exclusive contract arrangement that would waive fees for some patients with commercial insurance in exchange for a physician's other lab business (see Compliance Perspectives on the OIG's Advisory Opinion 15-04 on page 5).

This government scrutiny also serves as a reminder that labs must consider whether the anti-kickback statute is implicated any time they're making a payment, even arguably if it's to improve quality or reduce the physician's burdens, points out attorney Scott Grubman, former assistant U.S. Attorney now with Chilivis, Cochran, Larkins & Bever, LLP, Atlanta, Ga.

"Watch your Ps and Qs. These [deals] are being scrutinized," warns attorney Brian Flood, with Husch Blackwell in Austin, Texas.

To protect themselves, labs should consider these nine tips:

#1 Analyze any payment relationship with physicians to make sure that it's legitimate. Don't enter into a deal before carefully reviewing it and seeking legal counsel. "Look at an arrangement on the front end and see if the structure is okay. You can avoid a lot of heartburn later," says Grubman. Remember that if just one purpose of the deal is in exchange for patient referrals, that's enough to violate the anti-kickback law. If the overall arrangement does not make business sense absent the referrals, that's a huge issue, says Grubman.

"If there's any question, it's not worth it. This law is the most serious because of the criminal implications," he explains.

#2 Review "freebies" to physicians. Labs often give free items to doctors, but not all of them are legally okay, as noted by the seemingly contradictory advisory opinions that the Centers for Medicare & Medicaid Services (CMS) issued in 2013, finding one specimen collection kit a lab handed out lawful because it met an exception to the Stark law prohibiting these handouts but another kit violated the Stark law simply because of the different ways the specimens were collected. Don't assume that a particular specimen kit or other free item fits within the exception.

"If the documents only address how much a physician will make, it is hard to say that the intent was to improve care or other reasons."

—Brian Flood, Attorney

#3 If your proposed deal gets a clean bill of health, get that in writing from your attorney. That way you have documentation that you got a deal blessed. "It negates intent," explains Grubman. Unlike the Stark law, which is a strict liability statute, the anti-kickback law requires that you knew what you were doing was unlawful.

#4 Don't think that even a small deal or a small lab can fly under the radar. The government is increasingly using data mining to watch for spikes in bills and other changes. "As data [mining] gets more sophisticated, it can get outliers. The government can now pinpoint more granular subjects [such as physicians]. If a nail is sticking out of the floor they will hammer it down," explains Flood. In fact, as we have reported in GCA, CMS released significant data last April and reportedly intends to do the same again this year. See "Fraud and Abuse Implications of CMS Data Dump," in the April 2014 issue of *G2 Compliance Advisor*.

#5 Document the business reasons for the deal. "If the documents only address how much a physician will make, it is hard to say that the intent was to improve care or other reasons," explains Flood.

#6 Stay away from improper communication. "Don't let 'casual speak' color the deal. Dissuade conversations about [referrals from or perks to doctors]. Don't let that lie unchallenged," he adds.

#7 Beware of deals that carve out the federal health programs. The OIG has a "long standing concern" with such arrangements since they increase the likelihood of referrals for and overutilization of services involving Medicare and Medicaid patients even if the deal purports to only involve commercial business. A deal with such a carve-out may ironically cause it to receive greater scrutiny, rather than dodging that audit bullet.

#8 Don't forget your state law. Many states bar lease, fee-splitting and other arrangements between labs and physicians, even if they don't involve patient referrals.

#9 Watch for other legal actions that could trigger a government investigation. For instance, Cigna's lawsuit against HDL for waiving copayments could spark the interest of the OIG or other insurers to investigate the same issue. The routine waiver of copayments, coinsurance and deductibles to induce referrals is also an unlawful kickback.

"Caution is the right advice for the industry," says Flood.

Takeaway: Make sure your compliance department closely scrutinizes all arrangements between your laboratory and physician referral sources.

News at a Glance

Arizona Allows Lab Testing Without Doctor Order: Beginning in early July, Arizona residents will be able to order any laboratory test they want without a doctor's authorization, under a new law signed by Governor Doug Ducey on April 6. The new law does not require laboratories to perform the test nor does it require insurance companies to pay for the testing. Further, it specifically assigns any liability associated with testing or outcomes to the patient ordering the test. The law requires the performing laboratory to include a statement on the test result, in bold type, saying it is the responsibility of the person who was tested to arrange with their health care provider for interpretation of the results. Theranos, a laboratory testing company based in Palo Alto, Calif., supported the law throughout the legislative process. Theranos chief executive Elizabeth Holmes spoke at the signing ceremony that was conducted inside a Theranos local site. The company claims its testing technology allows smaller samples and lower prices than traditional laboratories—prices that Theranos has no problem sharing publicly. Theranos sells tests at 41 Walgreens drug store clinics. According to information provided by Theranos, 27 states, not including Arizona, and the District of Columbia allow consumers direct access to laboratory testing. There are 13 states that prohibit direct access for consumers. Generally, doctors and traditional laboratories do not support unlimited consumer direct access to testing.

HHS OIG Collaborates With Industry Leaders on Compliance Oversight: On April 20, the U.S. Department of Health & Human Services' Office of Inspector General (OIG) announced the release of a document, developed with the collaboration of leading industry trade groups, to offer guidance to governing boards of health care companies regarding their oversight of compliance plans. The American Health Lawyers Association, the Association of Healthcare Internal Auditors and the Health Care Compliance Association co-authored the guidance which highlights the audit, compliance and legal roles in comprehensive and effective compliance programs. According to the press release, the 19-page document is an educational resource that will benefit compliance officers, compliance auditors and legal counsel in addition to the boards to which they report, providing practical ideas, tools and tips on topics such as compliance policies, compliance reports to the board, and identifying compliance risks. It is meant to be flexible so its advice can be applied by boards of all sizes. The document, titled "Practical Guidance for Health Care Governing Boards on Compliance Oversight," can be found on the OIG's and the collaborating organizations' websites.

Lawsuit Win Invalidates RAC Payment Terms, Delays Contract Renewals: When the Centers for Medicare and Medicaid Services (CMS) put out its Request For Quotes to renew contracts with Recovery Audit Contractors (RACs) for 2014, it included some changes to the way RACs are paid and was sued by CGI Federal, Inc. (CGI) as a result. CGI contends that the new payment provisions, that change the payment timing from the first level of appeal to the second level of appeal, is inconsistent with commercial practice as is required by the Federal Acquisition Regulations. This change has the potential to delay payments to more than 400 days. In a recent ruling by the United States Court of Appeals for the Federal Circuit, the new payment provisions were invalidated, delaying the award of contracts until CMS either deletes the new payment terms or seeks a waiver to include them, which will delay the contract awards even further. G2

 G2 Compliance Advisor (ISSN 2332-1474) is published by G2 Intelligence, Plain Language Media, LLC, 15 Shaw Street, New London, CT, 06320. Phone: 1-888-729-2315 or Fax: 1-855-649-1623. Web site: www.G2Intelligence.com.

Kelly A. Briganti, JD, Editorial Director, Kelly@plainlanguagemedia.com; Barbara Manning Grimm, Managing Editor; Christopher Young, Editor; Avery Hurt, Contributing Writer; Marla Durben Hirsch, Contributing Writer; Stephanie Murg, Managing Director, G2 Intelligence; Kim Punter, Director of Conferences & Events; Randy Cochran, Corporate Licensing Manager; Jim Pearmain, General Manager; Michael Sherman, Marketing Director; Pete Stowe, Managing Partner; Mark T. Ziebarth, Publisher. ***Receiving duplicate issues? Have a billing question? Need to have your renewal dates coordinated? We'd be glad to help you. Call customer service at 1-888-729-2315.***

