G2 INTELLIGENCE
A DIVISION OF PLAIN LANGUAGE MEDIA

G2 Compliance Advisor

For Clinical and AP Laboratories and Pathology Practices

June 2017

INSIDE THIS ISSUE

www.G2Intelligence.com

Upcoming Events

Lab Institute 2017
October 25-27
Hyatt Regency Washington on Capitol Hill, Washington, DC
www.labinstitute.com

Enforcement Trends: Clinical Laboratories Continue to Figure Less Prominently in New OIG Enforcement Report

The Office of Inspector General just published its most recent Semiannual Report to Congress. To the untrained eye, the newest OIG Report, which covers Oct. 1, 2016 through March 31, 2017, is not substantially different from what we have come to expect. But there are some subtle differences, particularly with regard to labs.

Labs in Cameo, Not Leading Role

Laboratory and pathology testing remains on the OIG's radar, of course. Accordingly, the new OIG Report includes the customary section about the labs that got busted. The differences have more to do with volume than substance. There are only two items directly involving labs in the OIG Report, roughly 50 percent below previous norms for these reports. Conspicuous by their absence are mentions of problem areas involving or enforcement initiatives specifically targeting labs. This little subtlety represents a continuation of recent patterns, as illustrated by the chart below.

Continued on page 9

Compliance Perspectives: 10 Traps to Avoid When Investigating Potential Whistleblower Complaints

If one of your employees comes forward to report a billing, coding, reimbursement or other potential violation, the liability of your lab will turn on two critical questions:

1. Is the employee right?
2. Did you respond appropriately to the allegation?

Issue 1 is "sexier." But in the real world, it's Issue 2 that makes or breaks most *qui tam* whistleblower claims. An immediate, thorough and effective investigation is crucial to not only defending against *qui tam* claims but preventing employees from even bringing them in the first place. Unfortunately, investigations can be tricky and mistakes are easy to mistake. Here are 10 of the most common mistakes and what your lab should do to avoid them.

Continued on page 2

10 Traps to Avoid When Investigating Potential Whistleblower Complaints, *from page 1*

THE DUTY TO INVESTIGATE COMPLAINTS

Establishing procedures for fielding and responding to internal complaints is a central element of a laboratory compliance program. According to the OIG Model Compliance Plan for Clinical Laboratories, when labs learn about "potential violations or misconduct [involving their participation in federally funded health care programs], they must investigate the matter promptly.

The investigation is no mere formality. It is crucial for labs to determine if a violation has actually occurred so that they can take necessary steps to address the problem. The investigation also has to be accurate. False positives can expose your lab to needless penalties, not to mention bad publicity, for violations it did not actually commit; false negatives, on the other hand, can result in missed reporting and repayment deadlines, whistleblower lawsuits and higher penalties than your lab would have had to pay if it had self-disclosed.

Avoiding 10 Common Pitfalls

Although every situation is different, there are 10 common pitfalls that cause investigations to go wrong.

1. Rushing to Judgment

The Trap: Decades ago, the tendency was to downplay employee complaints and sweep them under the rug. But the rise of *qui tam* whistleblower lawsuits has changed attitudes in a big way. "We have gone from complacency to panic," according to one attorney who asked not to be named. "Labs are still rushing to judgment but now, instead of presuming that claims are baseless, the presumption is that they must be true." In addition to unnecessary self-reporting, premature self-condemnation sows chaos and costs innocent employees their jobs.

How To Protect Yourself: *Over*reacting to whistleblower claims is just as serious as underreacting to them. So do not rush to judgment one way or the other. Allow the investigation to run its course before deciding whether the allegation has merit and requires corrective action.

2. Failure to Screen Complaints before Investigating

The Trap: Whether out of spite or innocent mistake, employees are apt to use your lab's hotline to report transgressions that, even if true, are not violations, triggering costly, time-consuming and highly disruptive investigations that should have never been brought.

Example: A lab holds annual summer picnics for its client physicians where free hot dogs and burgers are offered. A lab employee complains that the arrangement is an illegal kickback. The lab reflexively launches an investigation and overlooks a crucial fact: gifts of nominal value like hamburgers and hot dogs do not violate anti-kickback laws. The investigation lasts a full week before sense is restored and it is called off.

How To Protect Yourself: First, you need to educate your employees about the compliance rules so they do not submit false reports. You also

G2CA

Glenn S. Demby, Editor

Lori Solomon, Contributing Editor

Catherine Jones, Contributing Editor and Social Media Manager

Barbara Manning Grimm, Managing Editor

David van der Gulik, Designer

Randy Cochran, Corporate Licensing Manager

Myra Langsam, Business Development

Michael Sherman, Director of Marketing

Jim Pearmain, General Manager

Pete Stowe, Managing Partner

Mark T. Ziebarth, Publisher

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

need a mechanism to filter frivolous complaints so that you do not automatically start an investigation every time the hotline rings.

3. Waiting Too Long to Start

The Trap: As a general principle, delaying an investigation complicates its work and undermines its reliability. Over time, memories fade, witnesses leave and physical evidence disappears. And in the health care fraud context, acting fast is imperative so that if the investigation does reveal wrongdoing you can comply with the deadlines to report it and make any necessary repayments to the government

One of the most common investigation mistakes is failing to consider all of the potential evidence.

How To Protect Yourself: Although you need to move fast, you cannot trade speed for fairness and thoroughness. Rushing an investigation is just as harmful as foot dragging.

4. Using a Biased Investigator

The Trap: One frequent mistake is allowing somebody with a personal interest in the case handle the investigation. The rule of thumb: The investigator's only agenda should be to determine the facts, not prove or disprove the charge.

How To Protect Yourself: Make sure the investigator is trustworthy, impartial and not related to or in any other special relationship with the accuser, accused or operation being investigated. Do not let supervisors investigate subordinates and vice-versa. Make sure the investigator doesn't have a personal or professional stake in the outcome, e.g., having your billing director investigate reports of improper billing and coding. If you can't find somebody objective and impartial within your organization, bring in an outsider to investigate.

5. Not Considering All of the Evidence

The Trap: One of the most common investigation mistakes is failing to consider all of the potential evidence.

How To Protect Yourself: There are two key sets of evidence your investigation must cover:

Witness accounts: Be sure to interview (or at least get written statements from) third parties that you have reason to believe can shed light on what happened. Third party testimony is especially crucial in he said/she said cases.

Documentary evidence: Other crucial evidence to consider in lab reimbursement investigations include documents like lab test requisition forms, physician correspondence, submitted claims and test reports.

6. Not Letting the Accused Confront the Accusations

The Trap: In cases where one employee accuses another of wrongdoing, it's not enough just to interview the *accuser*. You must also give the accused a chance to tell his/her side of the story. You also have to let them know exactly what they're accused of so they get a fair chance to respond.

How To Protect Yourself: Let the accused know exactly what they've been accused of doing and allow them to respond. However, it might be okay to

withhold the accuser's identity in some cases, e.g., where the accuser is a subordinate of the accused. It might also be not just appropriate but necessary to suspend or put the accused on temporary leave if his/her presence might intimidate witnesses or otherwise compromise the integrity of the investigation.

Doing an appropriate internal investigation isn't enough; you must also able to *prove* that your investigation was through, fair and impartial.

7. Asking 'Leading' Questions

The Trap: Interviews are a breeding ground for mistakes, including leading of witnesses—that is, phrasing questions in a way that cues the witness to respond in a certain way.

How To Protect Yourself: The investigator should draw up a list of questions before the interview and, if possible, submit it to counsel or somebody else knowledgeable about investigatory interviewing to verify that the questions are simple, properly phrased and free of cues that may inadvertently (or advertently) lead the witness.

- **Wrong:** "Did the employee accused of paying kickbacks ever say anything to you about offering free software to ordering physicians?"
- **Right:** "Did the accused ever say anything about marketing to physicians that you considered objectionable or inappropriate?"

8. Interviewing Witnesses in Front of Each Other

The Trap: Requiring accusers and other witnesses to tell their story in the presence of the accused (or other persons involved in the case) can be intimidating and damage the reliability of their testimony.

How To Protect Yourself: Be aware of and make efforts to control risks of witness collaboration and intimidation. At a minimum, make sure each witness is interviewed separately and not in the presence of other witnesses.

9. Not Following Your Own Investigation Procedures

The Trap: A surefire way to taint your investigation is to deviate from your lab's investigation procedures without explanation or justification.

How To Protect Yourself: Don't confuse the need for consistency and adherence to procedure for lack of flexibility and remember that there may be occasions where departing from standard routine is not only justifiable but necessary to ensure fairness.

10. Not Documenting Investigation

The Trap: Doing an appropriate internal investigation isn't enough; you must also able to *prove* that your investigation was through, fair and impartial.

How To Avoid It: Create an investigation report form that requires the investigator to list the steps taken, witnesses interviewed, etc.

Your first line of defense against fraud violations and misconduct is a great lab compliance policy. But policies can only do so much. Sooner or later, you're probably to face an allegation from one of your employees. At that moment, it's critical that you, as lab director, ensure that everyone stays calm and refrains from panicking into judgment until a fair and thorough investigation is carried out. Avoiding the 10 mistakes above will go a long way toward accomplishing that mission.

CASE OF THE MONTH

The eClinicalWorks EHR Settlement—Big Fines & Unprecedented CIA Obligations

With all the money it generates, it was only a matter of time before Electronic Health Records (EHR) technology got caught up in the False Claims Act dragnet. (See the related story on EHR overpayments by the CMS on page 11.) A significant new case came down on May 31 when eClinicalWorks (ECW), one of the country's biggest EHR software vendors agreed to pay $155 million to settle false claims charges for allegedly misrepresenting the capabilities of its product

The Justice Department claims that ECW cheated its way to certification by not telling the certifying entity that its EHR software didn't meet HHS criteria for accurate recording of user actions in audit logs, drug interaction checking and data portability.

EHR Certification, 101

Starting in 2009, HHS began making incentive payments to providers for demonstrating their "meaningful use" of certified EHR technology. To get their products certified, EHR vendors had to:

- Attest that the product meets HHS EHR criteria; and
- Pass testing by an independent, HHS-approved certifying entity.

The ECW Case

The Justice Department claims that ECW cheated its way to certification by not telling the certifying entity that its EHR software didn't meet HHS criteria for accurate recording of user actions in audit logs, drug interaction checking and data portability. To further the deception, ECW allegedly used "hardcoding" to modify its software before certification testing to ensure it would pass.

Result: The software was falsely certified. And because of that, provider claims for "meaningful use" incentives based on ECW's EHR software constituted false claims for which ECW was responsible.

Although it denies the charges, ECW has decided that settlement is wiser than resistance. At $154.92 million, the settlement is the largest False Claims Act recovery in the District of Vermont and may even be the largest financial recovery in the history of the State of Vermont, according to the DOJ press release. Here is how the bill will be divvied up:

- Three of ECW's founding members, including its CEO and medical director are jointly and severally liable for all $154.92 million;
- One of the software developers will pay a separate $50,000 out of his own pocket; and
- Two of the software's project managers will pay $15,000 apiece.

The Corporate Integrity Agreement

The damages are only part of the story. Arguably, the most significant and groundbreaking aspect of the settlement is the Corporate Integrity Agree-

ment. Five-year CIAs are par for the course in settlements of these cases. But the ECW includes some innovative elements designed to clean up the mess and ensure it does not happen again, including ECW's obligation to:

- Retain an Independent Software Quality Oversight Organization to assess the firm's software quality control systems and issue written semi-annual reports to the OIG;
- Provide prompt notice to its customers of any patient safety issues that may result from not telling the truth about its EHR software;
- Maintain a comprehensive list of such safety issues and steps mitigate them on its customer portal;
- Offer customers updated versions of the EHR software free of charge;
- Offer customers the option of having ECW transfer their data to another EHR software vendor without penalties or service charges; and
- Retain an Independent Review Organization to ensure that its provider arrangements comply with the Anti-Kickback Statute.

[For more details about the ECW case, see *United States ex rel. Delaney v. eClinialWorks LLC*, 2:15-CV-00095-WKS (D. Vt.)]

HIPAA SCORECARD

Health data and information security figured prominently in recent enforcement activity. In addition to the blockbuster eClinicalWorks EHR software settlement discussed on page 5, there was an unusually high volume of HIPAA enforcement action. Here is a Scorecard summary of three big HIPAA cases that were reported in May.

DATE	PROVIDER	ENFORCEMENT ACTION	ALLEGED VIOLATION(S)
May 10	Memorial Hermann Health System (Texas, non-profit system comprised of 16 hospitals)	$2.4 million settlement and agreement to implement Corrective Action Plan	Disclosed a patient's PHI without authorization to another patient who presented a fraudulent ID card to office staff and then compounded problem by issuing press release about incident that lists the victim's name
May 30	St. Luke's-Roosevelt Hospital Center (part of Mount Sinai Health System in New York)	$387,200 settlement and agreement to implement Corrective Action Plan	Staff member improperly faxed HIV status, sexual orientation, mental health diagnosis, physical abuse, sexually transmitted disease and other PHI about a patient to his employer rather than sending it to requested personal post office box. Center should have been on guard especially since there had been previous incidents involving staff
May 31	Former employee of Tufts Health Plan (Boston area)	Three months in prison, three years of supervised release and $52,000 in restitution payments	Stole names, birth dates, Social Security numbers and other PHI of over 8,700 customers, most of them over age 65, as part of a scheme involving filing of false income tax returns to claim tax refunds and Social Security benefits

Labs IN COURT

A roundup of recent cases and enforcement actions involving the diagnostics industry

BLS Bribery Case Gets Criminal

Case: The massive federal crackdown against doctors who allegedly took bribes from New Jersey-based Biodiagnostic Laboratory Service (BLS) in exchange for Medicare test referrals continues to grow. On June 6, a federal jury indicted a pair of cardiologists with a Patterson, NJ practice for their role in the BLS scheme. One of the doctors allegedly received a $500,000 loan, a free trip to Florida for fishing and visiting strip clubs and other bribes from BLS. His wife was also indicted for setting up the sham company through which the bribes were funneled. The other doctor is accused of taking bribes in exchange for over $900,000 in lab referrals.

Significance: There have been 45 convictions in the BLS case so far, 31 of them physicians. But most of those prosecutions have been civil cases. The new case ups the ante with criminal charges. The Patterson cardiologists are only the fifth and sixth doctors indicted in the scheme.

Fraudster Gets Maximum 10 Years for Lab Billing Ripoff & Obstructing Investigation

Case: Speaking of criminal charges, the mastermind of a false billing conspiracy was sentenced to the maximum 10 years in prison; his accomplice got 37 months. The defendants pleaded guilty to creating testing "clinics" to bill Medicare for tests that were medically unnecessary or not actually performed. The sham bilked the government out of over $7 million in false claims.

Significance: he details are pretty egregious. The plot, which was apparently planned over a long period of time, involved paying marketers $80 to $100 cash to recruit Medicare beneficiaries to the clinics. Marketers used the money to pay the beneficiaries bribes and pocketed the rest. Adding injury to insult, the co-plotters tried to obstruct the investigation.

Pathologists Pay $601K to Settle Stained Specimens False Billing Charges

Case: The case began when an anatomical pathologist filed a *qui tam* whistleblower lawsuit against his North Carolina practice for allegedly billing Medicare for medically unnecessary tissue tests. The practice denied the charges. But after the government elected to take over the case, it decided that discretion was the better part of valor and agreed to settle for $601K—$120,200 of which will go to the pathologist. .

Significance: One of the government's accusations was that the practice applied special stains to test specimens without first giving pathologists a chance to review specimens stained with more routine (and less expensive) hematoxylin and eosin (H&E) stains. And under Medicare rules, the pathologist must first review the routine H&E stained specimen for the special stains to be deemed medically necessary. (For more on the case, see the G2 blog, June 6, 2017.)

Pathology Labs Pays $897K to Settle Off-Label Marketing of Cell Stain Tests

Case: Memphis providers conducted a multi-year campaign promoting their immunohistochemical mast cell tryptase stain test for its ability to definitively diagnose a condition known as "mast cell enterocolitis." The claims went beyond the test's FDA

approval and unsupported by evidence, according to the government. Rather than slug it out in court, the defendants agreed to fork over $897,640 to settle the case.

Significance: The case is a useful illustration of the interplay among FDA approval, medically necessary and false claims act requirements. Because the promoted use was off-label, the tests were deemed not medically unnecessary under Medicare. And billing Medicare for medically unnecessary tests would have made the providers guilty of submitting false claims.

COMPLIANCE CORNER

Fixing a Hole in Whistleblower Retaliation Protection

SITUATION

Fictional Laboratories (FL) plans to deliberately bill Medicare for tests it does not actually provide. To carry out the scheme, it orders Pathologist A to falsely attest that she performed the tests. When she refuses, the lab fires her. When Pathologist B gets wind of what happened, he files a *qui tam* whistleblower claim against FL. He, too, is summarily fired. Making FL's actions even more deplorable is the fact that the lab is part of a federal health agency.

QUESTION

Against which pathologist did FL commit illegal retaliation?

A. Pathologist A

B. Pathologist B

C. Both of them

D. Neither of them

ANSWER

B. As absurd as it seems, under current whistleblower laws only Pathologist B would have a valid retaliation claim against FL.

EXPLANATION

Both pathologists were clearly victims of retaliation. And the federal *Whistleblower Protection Act* is supposed to protect employees of federal agencies who get fired in retaliation for blowing the whistle. The problem is that the law contains a nasty loophole: It bans retaliating against an employee for bringing a whistleblower lawsuit but not for refusing to obey an order to break the law. As a result, as it is currently constituted, the Act protects Pathologist B but not Pathologist A.

But all of that is about to change. A new federal bill called *The Follow the Rules Act* is designed to fix the glitch by specifically extending whistleblower protection against retaliation to employees who refuse to obey an order that would require them to break the law. The House of Representatives passed the bill on May 2 and the Senate did likewise on May 25. It is now on the President's desk and is sure to be signed.

Takeaway: Good for Congress for recognizing and trying to plug the retaliation protection loophole. But the problem may still not be resolved. In fixing one quirk, The Follow the Rules Act may actually have created another. The problem is that the legislation is missing something pretty important, namely, clarification that the new protection from retaliation for disobeying an order to break the law applies retroactively.

Clinical Laboratories Continue to Figure Less Prominently in OIG Enforcement Report, *from page 1*

Lab-Specific Items in OIG Reports Since 2010

OIG Semi-Annual Report Version	Lab-Specific Enforcement Initiatives, Problem Areas and Cases Mentioned
2017 Part 1	2
2016 Part 2	4
2016 Part 1	4
2015 Part 2	5
2015 Part 1	5
2014 Part 2	5
2014 Part 1	3
2013 Part 2	1
2013 Part 1	6
2012 Part 2	3
2012 Part 1	5
2011 Part 2	3
2011 Part 1	4
2010 Part 2	4
2010 Part 1	6

Here is a quick overview of the key compliance takeaways in the new OIG Report.

1. Improper Payments

Improper payments continue their steady climb, totaling $96+ billion in FY 2016, including a reported:

- $284.1 million in Express Lane payments to potentially ineligible Medicaid beneficiaries who may not have been eligible;
- $10.6 million more in Express Lane payments to potentially ineligible Children's Health Insurance Program beneficiaries; and
- Over $26 million in payments to Medicare and Medicaid beneficiaries who were dead at the time they supposedly received the billed services.

Improper payments for services that shouldn't have been billed in the first place:

- $358.8 million of the total $438.1 million paid by Medicare for chiropractic (82 percent) were for unallowable services;
- At least $176 million in Medicaid payments to State Agencies for room and board costs under the HCBS Waiver Program; and
- $2.7 million for hearing aid devices replaced without cost to the hospital or beneficiary.

Medical device and pharmaceutical companies are getting a lot of the attention that the OIG used to concentrate on labs.

2. Problem Areas

The Report cites a pair of vulnerabilities and misaligned incentives that the OIG focused on during the period:

- The 2-midnight policy for determining inpatient/outpatient status for Medicare hospital billing; and
- The tripling of Part D catastrophic coverage spending, much of which attributable to new high-price drugs.

3. Enforcement Activities

Key enforcement numbers for the first half of FY 2017:

- $2.04 billion in total recoveries;
- 468 criminal actions;
- 461 civil actions; and
- 1,422 exclusions.

Key areas of enforcement cited in the Report included prescription drugs, care in non-institutional settings and grant fraud. Laboratories did not make the list.

4. Enforcement Against Labs

Medical device and pharmaceutical companies are getting a lot of the attention that the OIG used to concentrate on labs. Even so, labs continue to figure prominently in OIG enforcement activities. Several of the biggest cases cited in the Report involve labs, including:

- The $6.1 million paid by Pharmasan Labs, NeuroScience and founder Gottfried Kellermann to settle claims of falsely billing Medicare for urinary transmitter testing, including via the use of "shift factor" measurement methods not properly validated under CLIA rules; and
- The $1.3 million settlement by New Jersey-based MedNet for allegedly using "fee-for-service" and "direct-bill" agreements to pay hospitals and physicians for Medicare referrals.

Takeaway: For labs, the most important thing about the new OIG Semiannual Report is the relative lack of attention paid, at least compared to previous years. Although labs remain fixed on the OIG radar, the agency seems to be focusing more than ever on drugs, devices and state agencies.

OIG REPORT

CMS Dished Out $729.4 Million in Wrongful EHR Incentive Payments & We're Going to Get that Money Back

Wrongful payments of Electronic Health Records (EHR) incentives are at the focus of two of the month's biggest stories in health care compliance. The first came down on May 31 when the Justice Department announced that one of the biggest EHR software vendors in the country, eClinicalWorks, had settled false claims charges stemming from allegedly overstating the capabilities of its product. In addition to the $155 million price tag, the settlement is notable for the sweeping restrictions the Massachusetts-based vendor accepted under the associated Corporate Integrity Agreement. (See page 5 for a summary and analysis of the ECW settlement.)

Less than two weeks later came another EHR bombshell in the form of an OIG report suggesting that CMS made more than $700 million in EHR "meaningful use" incentive payments to providers.

By The Numbers

The June 12 OIG report can be summed up by its ominous title: "MEDICARE PAID HUNDREDS OF MILLIONS IN ELECTRONIC HEALTH RECORD INCENTIVE PAYMENTS THAT DID NOT COMPLY WITH FEDERAL REQUIREMENTS" (all caps theirs, not ours). Here are the report's key numbers based on an audit period from May 2011 to June 2014:

- **729,424,395:** Estimated amount of total EHR overpayments (based on $291,222 of actual overpayments identified as being made during the audit period);
- **12:** The percentage of the $6.093 billion in total EHR incentive payments that were made to providers who didn't actually meet meaningful use requirements; and
- **$2,344,680:** EHR incentive payments made for the wrong payment year to providers who switched from Medicaid to Medicare incentive programs.

What Went Wrong

According to the OIG auditors, the $729.4 million in overpayments because providers didn't maintain support for their attestations. Of the 100 eligible providers audited, 14 (with payments totaling $291.2K) weren't actually in compliance with meaningful use requirements. The report cites three types of deficiencies:

- Insufficient attestation support;
- Inappropriate meaningful use periods reported; and
- Insufficient use of certified EHR technology.

The OIG suggests that it wasn't all the providers' fault. "CMS conducted minimal documentation reviews, leaving the self-attestations of the EHR program vulnerable to abuse and misuse of Federal funds, the report concludes.

The CMS was also partly to blame for the $2.34 million in wrong payment year payments. The agency "did not have edits in place to ensure that eligible

providers who switched from one program to the other were placed in the correct payment year upon switching," according to the report.

What Happens Now?

The overpayments already made are water under the bridge—except for the 14 audited providers who received the $291.2K which the OIG now intends to take back. For everybody else, the impact of the report are the actions it recommends going forward, including:

- Get back the rest of the $729.1 million in wrongful EHR incentives by determining which other eligible providers received payments even though they didn't actually meet meaningful use requirements;
- Educate eligible providers about how to properly document self-attestation; and
- CMS implementation of edits to ensure that eligible providers don't get payments under both Medicare and Medicaid EHR incentive programs for the same program year.

About 12 cents of every dollar of the $6.1 billion in incentive payments to eligible providers for demonstrating "meaningful use" of certified EHR technology shouldn't have been paid, according to the OIG. But now that the problem and its causes have been identified, corrective measures will be taken and providers who received incentive payments they didn't deserve, which may include pathologists and labs, will have to pay back the money.