G2 INTELLIGENCE
A DIVISION OF PLAIN LANGUAGE MEDIA

G2 Compliance Advisor

For Clinical and AP Laboratories and Pathology Practices

May 2015

Inside this issue

www.G2Intelligence.com

Six Ways to Reduce Risk of Employee Turning 'Whistleblower' Against Your Lab

The False Claims Act is the government's most successful fraud enforcement tool, especially since whistleblowers—individuals who bring suspected fraud to the government's attention—are able to receive up to 30% of the money recovered from the violator.

The Department of Justice obtained a record $5.69 billion in settlements and judgments from fraud and false claims cases in fiscal year 2014, $2.3 billion of which involved fraud against the federal health care programs. Most of the cases, called *qui tam* actions, were initiated by whistleblowers who received $435 million out of the recoveries, according to the Department of Justice's announcement. The number of *qui tam* suits filed in 2014 exceeded 700 for the second year in a row. This does not even include the number of qui tam actions that whistleblowers file where the government opts not to join or "intervene" in the lawsuit and take over the investigation.

All providers, including labs, are at risk of becoming a defendant of a whistleblower lawsuit, and their frequency seems to be increasing. For instance, a dermatology practice and related dermatopathology laboratory operating in Georgia agreed in April to pay the United States more than $3.2 million plus interest to settle allegations they

Continued on page 9

Get Paid With Less Stress

Occasional denials from payers are just part of doing business for health care providers. But labs face challenges getting paid that clinicians don't. In this two-part series, you'll learn how to keep your rate of denials as low as possible, and what to do when payers refuse your claims.

Coding errors are one of the most common reasons for denials from payers, says Elizabeth Woodcock, president of the consulting firm Woodcock and Associates. However, in most cases, the coding will have been done by the physician's office that referred the patient or sent the samples to you. You can't do anything about problems with codes that your office didn't assign. Or can you?

"Labs get denials all the time because of incorrect diagnoses from the providers," says Tammie Olson of Management Resource Group, a firm offering financial management and support services

Continued on page 2

Get Paid With Less Stress, *from page 1*

for the health care community. "Often I see the lab sending queries back after the denial, but it might be better to screen for this and send queries back to the provider before submitting the claim. If the lab sees something specific that they know is not covered, then they really should query the physician for a better diagnosis before submitting the claim."

And if coding is very often the reason for denial, quite often the basis for the denial is that the test was "not medically necessary." This type of denial poses special challenges for labs. "Labs are generally at a disadvantage when it comes to demonstrating medical necessity. In a lab, you don't have a direct relationship with the patient, and you don't have access to the full records and history of the patient, so making sure your claims pass the 'medically necessary test' can be tricky," says Debbie Parrish, of Parrish Law Offices, a firm specializing in obtaining and protecting reimbursement for health care systems, physicians, and laboratories. But you don't have to just sigh and write off these bills. You have more control than you might think.

> ***"Often I see the lab sending queries back after the denial, but it might be better to screen for this and send queries back to the provider before submitting the claim. If the lab sees something specific that they know is not covered, then they really should query the physician for a better diagnosis before submitting the claim."***
>
> ***—Tammie Olson, Management Resource Group***

Being aware of the policies of the payers you typically work with (and these policies can vary a great deal from payer to payer, Woodcock points out) is crucial. "Before you bill for laboratory services, research your payers' websites for their reimbursement and billing guidelines," advises Olson. This way you'll know beforehand when your claim is likely to hit a snag.

Then you need to carefully review the diagnosis code. "Make sure that the diagnosis linked to the procedure is correct, specific, and accurate. For example, a doctor wouldn't order a CBC for someone with high cholesterol, but he or she might have to order one because the patient is taking a certain medication for high cholesterol that may cause adverse effects. So a more accurate diagnosis would be 'use of high risk medicine' and not 'high cholesterol.'" Often, though, the problem with the diagnosis is not lack of accuracy but lack of specificity. "Most insurance providers do not cover the code General Health Profile, CPT 80050, but it is a favorite of providers to order," says Olson.

Some situations are specific to Medicare claims. "Prior to running a test that is likely to be deemed not medically necessary by Medicare, you need to make sure that the provider has provided an ABN (advance beneficiary notice/Medicare waiver of liability) before you run the test. Otherwise, you will not be able to bill the patient if the claim is denied as not medically necessary," explains Olson. Providers are required to give Medicare patients this waiver of liability for any services they provide that may not be covered or are considered not medically necessary.

Of course making sure the coding is right and ABNs are available when they should be may take a little diplomacy. "Clinicians are busy, and tend to get cranky when asked to justify their clinical decisions. There is a fine line between getting the information you need and becoming a nuisance," says Parrish. Some labs find that bundling their queries is more effective than addressing them as they come up. Since you probably bundle

G2 Compliance Corner

Ensure Regular Training for Billing and Coding Staff

Don't overlook continual training of your billing and coding staff. It's a compliance principle that the OIG emphasized in its initial compliance guidance for laboratories in 1998 and it is still just as important today, particularly with changes such as ICD-10 on the horizon. One of the compliance officer's roles, according to the OIG's *Compliance Program Guidance for Clinical Laboratories*, is to develop and participate in a training program and ensure all appropriate personnel are knowledgeable about the compliance program and "pertinent Federal, State and private payer standards." That guidance document says an effective compliance program depends on "regular, effective education and training programs for all affected employees." So make sure you are training new staff and re-training existing staff on the laboratory's compliance program, fraud and abuse laws, billing and coding requirements, and claims submission.

Specifically, with regard to billing and coding, the OIG guidance says "for certain employees involved in the billing and coding functions, periodic training in proper CPT/HCPCs and ICD-9 coding and documentation should be required."

In a footnote the OIG emphasizes that coding responsibilities "create a greater organizational legal exposure, and therefore require specialized training" and advises laboratories to first fill coding positions with "individuals who have the appropriate educational background and training." Once you hire appropriate staff, the guidance recommends in a separate footnote that at least annual training be provided for general compliance issues with increased number of annual training hours specifically for staff involved with coding and billing functions. It also emphasizes the need to train new staff as soon as possible.

When deciding what to highlight in training, look not just to new developments but also enforcement trends and issues the OIG highlights in its annual Work Plan, new guidance, fraud alerts and other guidance documents. And after you've trained and retrained staff, make sure the compliance message stuck—the OIG's 1998 guidance says you should be auditing and monitoring your billing and coding compliance. Address any problem areas found in those audits with further training.

your claims as well, this should be relatively easy to fit into your workflow. The important thing is to know your clients and work with them with courtesy and respect. Once you make a habit of checking codes before you submit, and querying providers about any potential problems, you are likely to find a pattern to your denials. Once you've worked out the bugs with your providers, many of these will go away.

No matter how careful you are, though, some claims will bounce back. Next month, we'll talk about what to do when that happens.

Takeaway: Laboratories face unique challenges when it comes to claim denials but still have opportunities to reduce denials by taking steps before submitting to make sure claims are as clean as possible.

Update: New Study Credits Criminal Attacks as Source of Most Health Care Data Breaches

As we reported in our April issue, cybersecurity is gaining national attention thanks to notorious data hacks like Sony and Anthem, and now Premera. The President has drawn attention to the issue calling for legislation and sharing of information about security risks and incidents. Our April issue of *GCA* provided tips for taking action now to avoid cybersecurity incidents and highlighted a 2014 study by Ponemon Institute that 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.

The Ponemon Institute issued a new study in May 2015 indicating health care-related criminal attacks on data have increased 125 per cent since 2010 and are "the leading cause of data breach" in health care. Yet, the study also indicates most organizations are still not prepared to respond to this threat to security of patient health information. "We are seeing a shift in the causes of data breaches in the healthcare industry, with a significant increase in criminal attacks. While employee negligence and lost/stolen devices continue to be primary causes of data breaches, criminal attacks are now the number one cause," said Dr. Larry Ponemon, chairman and founder of the Ponemon Institute in a press release announcing the study.

"According to the FBI, criminals are targeting the information-rich healthcare sector because individuals' personal information, credit information and protected health information (PHI) are accessible in one place, which translates into a high return when monetized and sold."

—Fifth Annual Study on Privacy & Security of Healthcare Data, Ponemon Institute

The study involved 90 covered entities and 88 business associates and its findings revealed that over 90 per cent of health care organizations surveyed had at least one data breach over the past two years, and 40 percent had over five breaches in the prior two years. The authors estimated that such breaches create a $6 billion annual cost for the health care industry, with health care organizations incurring average costs per breach of $2.1 million, $1 million for business associates. Forty-five percent of study participants reported that criminal activity was behind their data breach and 12 per cent found "malicious insider" activity behind an attack. While the study reports that the "root cause" of data breaches "is shifting from lost or stolen computing devices to criminal attacks," "employee negligence remains a top concern when it comes to exposing patient data." Seventy per cent of participants indicated that employee negligence was their top concern, and the authors attribute this concern to the fact that many incidents involve not just lost or stolen devices but also malware attacks and phishing, which relate to employee failure to follow security procedures.

Despite these numbers, the study found that only 40 per cent of health care providers were worried about the risk of cyber attack and only 33 per cent believed they had "sufficient resources to prevent or quickly detect a data breach." Another study, from EiQ Networks that surveyed IT decision makers across industries, including health care, about information security, backs up these findings. That survey noted that 62 per cent of the professionals surveyed felt their organization had no process or only a "partial process" for detecting and responding to security incidents and only 15 per cent felt their staff were sufficiently prepared to identify and respond to a cyber attack.

This latest Ponemon study involved interviews of "senior-level personnel at healthcare providers" and expanded its scope to encompass business associates as well. HIPAA requires both covered entities such as laboratories and their business associates to protect patient's health care information. "According to the FBI, criminals are targeting the information-rich healthcare sector because individuals' personal information, credit information and protected health information (PHI) are accessible in one place, which translates into a high return when monetized and sold," Ponemon's press release indicates.

Ponemon's *Fifth Annual Study on Privacy & Security of Healthcare Data* can be obtained at www2.idexpertscorp.com/ponemon.

Takeaway: This latest study emphasizes that the health care industry faces a significant threat to security of patient information and laboratories and other health care organizations need to ramp up efforts to protect patient information. G2

Enforcement and Guidance Efforts Serve as Reminder: Re-evaluate and Update Your Compliance Plans

Laboratories should revisit their compliance programs now that the government has released its latest report on the success of its fraud-fighting efforts as well as new compliance guidance for health care governing Boards.

The Departments of Justice (DOJ) and Health and Human Services (HHS) recently revealed that their fraud prevention and enforcement efforts recovered $3.3 billion in taxpayer dollars in fiscal year (FY) 2014. For every dollar spent, the government recovered $7.70, an "extraordinary" return on investment, according to the Departments' joint announcement. They will continue to escalate their efforts, using increased funding, new authority granted by the Affordable Care Act, more real-time data analytics, and continued use of the False Claims Act, which provided $2.3 billion in civil settlements and judgments involving claims against the Medicare and Medicaid programs in FY 2014.

> ***"This most recent document is a tool to [help] governing Boards responsibly carry out their compliance oversight obligations, and is applicable across the health care industry."***
>
> **—Katherine Matos, Office of Counsel for the Inspector General**

In addition, on April 20, HHS' Office of Inspector General (OIG) released a compliance guidance document created through the joint efforts of the OIG, the American Health Lawyers Association (AHLA), the Association of Healthcare Internal Auditors (AHIA) and the Health Care Compliance Association (HCCA). The document, titled *Practical Guidance for Health Care Governing Boards on Compliance Oversight*, assists governing Boards of health care entities in their oversight of compliance plans.

While the intended audience of the new tool is governing Boards, the document offers anyone with a compliance role insight and ideas for improving compliance within their laboratory or other health care organization. According to a press release, the 19-page document is an educational resource that will benefit compliance officers, auditors and legal counsel in addition to the Boards to which they report and can be adapted for organizations of all sizes.

The guidance is the OIG's latest advice for health care Boards, since its last offering in 2012, titled "Toolkit for Health Care Boards." "OIG seeks to provide meaningful guidance to the public on a variety of issues. We published three previous guidance documents regarding Board governance [in conjunction with AHLA, see Box, p. 8] but much has changed since that time," Katherine Matos, senior counsel, Office of the Counsel for the Inspector General, explains.

In addition, while prior guidance documents included suggested questions for directors or areas of inquiry, this new guidance includes tools and tips and provides "practical ideas that Boards can use," Matos points out.

"This most recent document is a tool to [help] governing Boards responsibly carry out their compliance oversight obligations, and is applicable across the health care industry," she adds.

The introduction explains: "A critical element of effective oversight is the process of asking the right questions of management to determine the adequacy and effectiveness of

the organization's compliance program, as well as the performance of those who develop and execute that program and to make compliance a responsibility for all levels of management." The guidance also explains the interrelationship between and individual importance of the following compliance functions: compliance, legal, internal audit, human resources and quality improvement.

The areas of focus addressed in the guidance include: expectations for Board oversight, compliance roles, reporting to the Board, identifying and auditing risk areas, and encouraging accountability. The document recommends using existing guidance materials available to Boards and compliance professionals as "benchmarks" for evaluating the effectiveness of their compliance plans—including the Federal Sentencing Guidelines, OIG compliance program guidance and Corporate Integrity Agreements (CIA). While a CIA is an agreement that entities enter into once they have already gotten in trouble, the measures negotiated into these agreements "may be helpful resources for Boards seeking to evaluate their organizations' compliance programs," the guidance says.

Suggestions for facilitating management's compliance reporting directly to governing Boards include use of dashboards and executive sessions and the document discusses methods for keeping tabs on current compliance risks, including sources such as compliance hotlines and internal audits as well as "professional organization publications, OIG-issued guidance, consultants, competitors, or news media." The guidance also advises: "When failures or problems in similar organizations are publicized, Board members should ask their own management teams whether there are controls and processes in place to reduce the risk of, and to identify, similar misconduct or issues within their organizations."

It's worth noting that among the top risk areas highlighted, the first issue mentioned is referral relationships and arrangements—an issue of significant relevance to laboratories particularly in light of last year's fraud alert and current enforcement efforts targeting such relationships. Other risk areas highlighted were billing, privacy breaches and quality-related events.

Highlighting the potential for "new incentives and compliance risks" created by current health care reform efforts, the guidance notes: "New payment models have also incentivized consolidation among health care providers and more employment and contractual relationships (e.g., between hospitals and physicians)." Laboratory compliance professionals should heed the guidance's suggestion that "Boards of entities that have financial relationships with referral sources or recipients should ask how their organizations are reviewing these arrangements for compliance with the physician self-referral (Stark) and anti-kickback laws."

The guidance also highlighted increasing transparency, with the availability of data from CMS on quality measures, payment data and the Sunshine rule providing public access to more information than ever before. The OIG and its collaborators encourage Boards to "consider all the beneficial uses of this newly available information" for evaluating compliance and establishing benchmarks. Finally, Boards are urged to consider and employ measures to incentivize compliant behavior and create a culture of compliance, while conducting self-evaluations and, when necessary, self-reporting non-compliance and repaying overpayments.

"We hope Boards will view this document as a toolkit, and use the practical tips included to foster enterprise-wide compliance within their organizations," says Matos.

COMPLIANCE PERSPECTIVES

> *"The compliance program guidance documents are directed to present a set of industry-specific guidelines for consideration when developing or implementing a compliance program."*
>
> —Katherine Matos, Office of Counsel for the Inspector General

The new Board guidance is also meant to dovetail with the OIG's existing specific compliance guidances for labs and other providers, which the OIG issued in 1998 but which the OIG still relies on today. That guidance is designed to establish a culture of compliance that promotes prevention, detection and resolution of instances of unlawful conduct or activities that are against a lab's ethical and business policies.

"The compliance program guidance documents are directed to present a set of industry-specific guidelines for consideration when developing or implementing a compliance program. Since management generally develops and implements the compliance program, this [lab-specific] document is most helpful for them, although Boards may also review these documents as part of their self-education," says Matos.

The OIG's compliance guidance is technically "voluntary." However, having and using a compliance program can not only prevent billing and other problems; it can also demonstrate good faith if a problem is uncovered internally or during an investigation and thereby reduce or avoid penalties. A compliance program also helps a lab minimize loss, identify and prevent wrongful conduct, and develop methodologies that encourage employees to report potential problems, according to the guidance.

Evidence that compliance programs reduce risks, save money

Compliance programs do bear fruit. For example, Houston, Texas-based Memorial Hermann Hospital System recently learned that one of its employees had embezzled the System out of nearly $10 million over 14 years in a false invoicing scheme. But the System only learned of the embezzlement because the system's chief compliance officer had received an anonymous letter alerting him to it. Had there not been a compliance officer and an effective line of communication to that officer, the letter writer may not have known where to turn and opted not to reach out, and if sent, the letter could have ended up languishing in the mail room or someone's inbox. Both the special lab compliance guidance and the new governing Board guidance note the importance of communicating clear reporting mechanisms as an essential element of an effective compliance program. The employee has been arrested for defrauding his employer and reportedly pleaded guilty April 22. He faces up to 20 years in prison and payment of up to $250,000.

In addition, virtually all of the agreements between providers and the OIG to settle instances of fraud, abuse and improper billing pursuant to the OIG's voluntary self-disclosure protocol are the result of the provider's use of an effective compliance program, which unearthed a problem the provider then brought to the OIG's attention, rather than ignoring or hiding it. Settlements made under the self-disclosure protocol typically cost the provider much less than had the provider not self-disclosed and the government had learned of the improper billing from another source. Moreover, in most instances the OIG won't impose a CIA on the entity that came forward, according to the OIG's latest guidance about its protocol.

COMPLIANCE PERSPECTIVES

Time to take the plunge: Review your program for deficiencies

Many lab compliance programs may be due for a tweaking or even an overhaul. Before forging ahead, consider these four tips:

1. Review your compliance program against the OIG's recommendations and fill gaps where needed. For instance, make sure that employees and others know how to report a suspect activity and that the lab communicates that complaints and reports will be promptly investigated. While it was beneficial for Memorial Herman to receive a letter tipping it off to an employee's embezzlement, arguably its compliance program could do with some fine tuning, since the scheme went on for 14 years before it was discovered.
2. Integrate into your compliance program some of the practical suggestions from the OIG's new guidance to governing Boards, such as measures from recent CIAs. For instance, ensure you implement a vigorous employee training program, develop written standards and policies, appoint a compliance officer and compliance committee, and avoid employment of persons ineligible for participation in the federal health care programs.
3. Make sure that the lab's compliance program incorporates more recent requirements, such as fraud alerts and advisory opinions pertaining to lab arrangements with physicians (See "Compliance Perspectives: OIG Advisory Opinion Makes Convenience and Efficiency Suspect," *G2 Compliance Advisor*, April 2015, p. 5; "Compliance Perspectives: OIG Warns of Anti-Kickback Statute Violations in Laboratory Payments to Referring Physicians," *G2 Compliance Advisor*, July 2014, p. 5).
4. Keep an eye out for further developments. For example, the Affordable Care Act requires providers to operate compliance programs. HHS has solicited information on what those mandatory programs should entail but has not yet issued rules implementing this provision. While it's expected that the required programs will look similar to the OIG's current compliance guidance or at least incorporate some of those provisions, the new rules may require labs to modify their programs down the road accordingly.

Takeaway: Use tips in the new guidance for health care governing boards to evaluate effectiveness and adapt compliance plans to a changing health care environment.

Resources for Evaluating Effectiveness of Compliance Programs

As the new OIG/AHLA/AHIA/HCCA guidance for governing boards suggests, laboratories and other health care organizations have a wealth of resources available to help them ensure they are implementing effective compliance programs. The joint guidance issued this year is only one of a series of resources the OIG offers specifically for Health Care Boards. Just because they target governing boards doesn't mean they aren't equally useful for compliance officers and others looking to ensure compliance. The following three preceding joint guidance efforts can be found on the OIG's website:

- "Corporate Responsibility and Corporate Compliance: A Resource for Health Care Boards of Directors," AHLA and OIG, April 2, 2003 (in the wake of the Sarbanes-Oxley Act, this resource helps health care boards "establish, and affirmatively demonstrate, that they have followed a reasonable compliance oversight process").
- "An Integrated Approach to Corporate Compliance: A Resource for Health Care Boards of Directors," AHLA and OIG, July 1, 2004 (addressing roles of in-house counsel and the chief compliance officer "in supporting the compliance oversight function of health care organization governing boards").
- "Corporate Responsibility and Health Care Quality—A Resource for Health Care Boards of Directors," AHLA and OIG, Sept. 13, 2007 (continuing the focus on compliance oversight but adding an emphasis on oversight of health care quality and patient safety as well in response to "a new era of focus on quality and patient safety").

For more resources helpful in evaluating compliance programs, see the box on page 11.

Six Ways to Reduce Risk of Employee Turning 'Whistleblower' Against Your Lab, *from page 1*

violated the False Claims Act by engaging in improper financial relationships with some of its employed physicians and improper billing for dermatopathology analyses performed by the lab. The litigation was brought by three physician whistleblowers, who will receive more than $584,000 from the recovery for their efforts. The April 2015 settlements with Health Diagnostic Laboratory and Singulex for $48.5 million also stem from whistleblower lawsuits. (See "HDL, Singulex Agree to Settle AKS, FCA Charges for $48.5 Million," *G2 Compliance Advisor*, April 2015, p. 1.) The Department of Justice has not made public the amount that those whistleblowers will receive from the recovery amounts.

> ***"Providers need to treat everyone as a potential whistleblower."***
>
> ***—Scott Grubman, attorney, Chilivis, Cochran, Larkins & Bever, LLP***

"Whistleblowers are the government's police," notes David Zetter, president of Zetter Healthcare Management Consultants in Mechanicsburg, Pa. and a member of the National Society of Certified Healthcare Business Consultants (NSCHBC).

Most whistleblowers, also called "relators," are current or former employees (or otherwise affiliated with the provider, such as a contractor or business partner) who become frustrated or disgruntled and take action accordingly. "Providers need to treat everyone as a potential whistleblower," says attorney Scott Grubman, former U.S. assistant attorney now with Chilivis, Cochran, Larkins & Bever, LLP, Atlanta, Ga.

Since whistleblower suits alleging violations of the False Claims Act are filed under seal, a lab may not know for months or even years if someone has filed one against it. By the time the lab learns about it, the investigation into its operations may be nearly complete.

Six ways to keep an employee from blowing the whistle on your lab

You're much better off avoiding and preventing a whistleblower suit than defending one. Luckily there are some steps you can take to reduce this risk:

#1. Make sure employees and others have an opportunity to communicate compliance concerns. An employee who can raise a concern and have it investigated by the lab internally is less likely to feel ignored and feel the need to take further action, says Zetter. You can use a locked suggestion box, an "open door" culture and other methods to encourage communication. "One of the best investments a provider can make is a compliance hotline. I think this makes employees feel that their concerns matter, it forces providers to evaluate potential problems early on, and it looks good to the government, if you wind up getting on its radar anyway," says Grubman.

#2. Investigate the concern being raised. Don't ignore a billing, patient safety or other concern that's been brought to the lab's attention. If a problem does exist, correct it. It's a lot harder for a whistleblower to prevail if you can show that you took the concern seriously and took action to fix it, says Grubman.

#3. Make sure to get back to the person reporting, if known. You don't have to necessarily inform the person of the nature or result of the investigation (and in some instances you won't want to, since some actions, such as employee discipline, are confidential) but at least communicate that you're addressing the issue, says Zetter. If you don't, that person is less likely to report a problem the next time—or report it elsewhere to a more sympathetic ear.

#4. Keep an eye out for unusual employee activity. For instance, employees who are unusually inquisitive about issues not within their job responsibilities or come in after hours or on weekends may be gathering documents and other information to back up a *qui tam* action.

#5. Conduct employee exit interviews with employees leaving employment, and ask about any compliance concerns. If the employee states that he is unaware of any issues, document that response, to reduce the risk that the employee may turn around and become a whistleblower—since he has claimed he knew of no compliance issues. If the employee does raise a compliance concern, the lab needs to investigate it, says Zetter.

#6. Be careful about terminating someone who has complained or brought an issue to the lab's attention. This is especially true if the employee feels that the lab didn't adequately address the complaint. The employee may be vindictive, and may take his complaint to the government. "Don't fire or discipline someone just because he or she brought a potential issue to your attention. Not only will this drastically increase the chances that the person will become a whistleblower, but it is illegal retaliation under the False Claims Act," says Grubman.

Takeaway: Labs should be on alert that private citizens can file a lawsuit claiming the lab has improperly billed the federal health care programs in violation of the False Claims Act. Make sure that your lab has an effective compliance program to reduce the risk that any improper billing is occurring and to correct it if detected. G2

Whistleblowers Can Offer Statistical Sampling to Support Fraud Claims

A federal trial court in Florida has ruled that qui tam or whistleblower plaintiffs can use statistical sampling to prove fraud in a False Claims Act lawsuit. The court explained:"[N]o universal ban on expert testimony based on statistical sampling applies in a *qui tam* action (or elsewhere), and no expert testimony is excludable in this action for that sole reason…."

The whistleblower in this case had brought claims against entities that operated facilities at which she had worked, claiming they defrauded the U.S. and Florida governments by upcoding or upcharging for services rendered. Arguing that it was too difficult to provide individual analysis of claims from 53 facilities, the plaintiff asked the court to admit expert testimony about statistical sampling she planned to provide. The sampling had not yet been performed but the plaintiff wanted to determine if the court would accept such evidence to prove falsity of claims.

History of the case. The defendants had previously succeeded in getting the claims dismissed because the alleged fraud wasn't stated with sufficient particularity. Federal Rules of Civil Procedure require that fraud allegations be stated with particularity—that is, with specific detail. The plaintiff had claimed in her original complaint that she "witnessed false claims submissions and 'flagrant upcoding'" of Medicare and Medicaid claims. The court ruled that she had alleged only a "general scheme to defraud the government" and described only one instance of fraud without giving "'details about the fraudulent substance of the submission or about the time of the submission or about the government's overpaying the claim.'" It ordered the plaintiff to file an amended complaint with more specific details to describe the alleged

fraud—including "'who, what, when, and where.'" The government chose not to intervene in the whistleblower's case. The defendant refiled the complaint naming more defendants and claiming fraud occurred at 53 facilities—including facilities the plaintiff hadn't visited.

Sampling evidence. In support of her amended complaint, Plaintiff claimed gathering specific evidence of fraud from all 53 facilities and some off-site storage facilities was impossible. Therefore, she proposed using expert testimony based on statistical sampling to prove falsity of claims. The expert alleged that the sampling would estimate the total overpayments: "For example, if 1% of the population is sampled and reviewed, the total overpayment in the population is probably about 100 times the overpayment in the sample."

Court's reasoning. The court relied on a case from a Tennessee district court in 2014 that allowed statistical sampling due to the "large universe of allegedly false claims" making it "impracticable for the Court to review each claim individually" without using "an unacceptable portion of the Court's limited resources." It also cited a Kentucky case decided earlier this year which allowed statistical sampling.

The court rejected defendants' arguments that sampling isn't allowed in a qui tam action. The court denied the motion to admit the expert testimony that didn't yet exist but unequivocally said such testimony, once it did exist, wouldn't be excluded simply because it was based on statistical sampling. Defendants also argued that because the plaintiff was bringing the request before the sample was even conducted, the defendant couldn't challenge the margin of error. The court left open the possibility of defendants' successfully challenging the appropriateness of the sampling and the margin for error once the sampling was performed, stating "defects in method, among other evidentiary defects, might result in exclusion."

Takeaway: While this latest decision didn't rule on the admissibility of specific sampling evidence, the court made an unequivocal statement that such evidence can be used to prove fraud in qui tam false claims lawsuits. G2

Resources Helpful in Evaluating Compliance Programs

The government has provided several helpful resources that can help laboratories and other healthcare providers evaluate the effectiveness of their health care programs. Here are just a few of those resources:

- United States Sentencing Commission, Federal Sentencing Guidelines, Organizational Guidelines (Chapter 8) (available at www.ussc.gov).
- "Compliance Program Guidance for Clinical Laboratories," OIG, 63 Fed. Reg. 45076; Aug. 24, 1998 (available on the OIG website oig.hhs.gov under the Compliance tab).
- "Handout: A Toolkit for Health Care Boards," OIG, Feb. 27, 2012; "The Health Care Director's Compliance Duties: A Continued Focus of Attention and Enforcement," OIG, Aug. 29, 2011 (both available on the OIG website under the Compliance tab and subsection "Compliance 101" under the heading compliance documents for governing boards).
- Corporate Integrity Agreement Documents (agreements between the Office of Inspector General and entities alleged to have compliance violations; these documents include measures the organizations have been required to implement to address compliance issues; available on the OIG website under the Compliance tab).
- Self-Disclosure protocol (information about self-disclosing evidence of potential fraud; available at the OIG website under the Compliance tab).
- Advisory Opinions, Special Fraud Alerts, Bulletins and other Guidance, such as the Advisory Opinion 15-04 addressing agreements to waive fees for out-of-network patients and the 2014 Special Fraud Alert regarding payments to referring physicians (all available under the Compliance tab on the OIG website).

News at a Glance

CAP and ADASP Recommend Secondary Review of Anatomic Pathology Cases: The College of American Pathologists (CAP) and the Association of Directors of Anatomic and Surgical Pathology (ADASP) have developed a "new evidence-based guideline to provide recommendations for secondary and timely reviews of surgical pathology and cytology cases to improve patient care."

The guideline, titled "Interpretive Diagnostic Error Reduction in Surgical Pathology and Cytology," was published on the website of the *Archives of Pathology & Laboratory Medicine* as an Early Online Release. The guideline addresses the analytical phase, in which pathologists use "inherent judgment" while interpreting slides. CAP and ADASP created an expert panel of pathologists which studied the potential for errors during this phase.

The panel made five recommendations which call for institution of secondary review by another pathologist, on a timely basis but ideally before diagnosis; suggest reviews should be devised to accommodate the circumstances of the specialty or pathology group and be documented; and advise results should be monitored and changes instituted to address areas of disagreement or error. The guideline will be reviewed every four years unless new evidence arises that could substantially impact the guideline recommendations.

Individuals Sentenced for Diagnostic Testing Schemes: Yet another physician has been sentenced in connection with the Biodiagnostic Laboratory Services LLC (BLS) case. Franklin Dana Fortunato of Montville was sentenced to 14 months in prison with a year supervised release and a $75,000 fine and $635,0000 forfeiture. He previously had admitted accepting bribes in exchange for referral of blood specimens and pleaded guilty to violating the federal Travel Act and filing a false tax return. Fortunato admitted he didn't declare the bribes as income. The government alleged he failed to pay $160,000 in taxes for the undeclared bribes and other payments such as patient co-pays and funds received from other providers. So far, 38 individuals—including 26 physicians—have pleaded guilty in this case.

In a separate matter, the owner of another New Jersey diagnostic testing facility, Vijay Patel, was sentenced to 12 months in prison after having pleaded guilty to one count of health care fraud for submitting Medicare claims for diagnostic testing services that a cardiologist had performed. The U.S. Attorney explained the cardiologist performing the services was subject to pre-payment review and avoided such review when Patel submitted the claims as if his diagnostic testing facility had performed the services. The government said Patel kept part of the payment received and remitted the rest to the cardiologist.

Palmetto GBA Issues Proposed Draft LCD for Oncotype DX® Prostate Cancer Assay: Prostate cancer testing has received significant attention lately as the industry seeks to find reliable ways of identifying the appropriate treatment strategy for patients diagnosed with such cancer. Recognizing the difficulty in distinguishing patients needing aggressive treatment and those that could be observed, Palmetto is proposing coverage of an assay that measures cancer aggressiveness. The proposal would cover the Oncotype DX® if there's been a "needle biopsy with localized adenocarcinoma of prostate," the patient's stage is either very low risk disease or low risk disease, there's a life expectancy of 10-20 years and other conditions are met. The patient's medical record must demonstrate medical necessity for the services. The comment period ends July 24, 2015. 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.***

