G2 INTELLIGENCE
A DIVISION OF PLAIN LANGUAGE MEDIA

LAB Compliance Advisor

For Clinical and AP Laboratories and Pathology Practices

October 2021

IN THIS ISSUE

www.G2Intelligence.com

From the Bench: Courts Create New Defense for False Claims Based on Reasonable Mistakes about Regulatory Requirements

The *False Claims Act* (FCA) bans labs and other providers from "knowingly" submitting false claims. "Knowingly" is a curious word. Medicare coverage and billing rules can be intricate, confusing and hard to understand. So, in a different world, "knowingly" might provide legal cover to labs and other providers that want and try to comply but can't figure out what exactly the rules require. However, courts, prosecutors and investigators have interpreted "knowingly" very broadly to ensure that confusion over the rules isn't a defense. But recently, federal courts in some parts of the country have been begun recognizing misinterpretation of regulatory requirement as a valid defense, as long as the mistake is reasonable. Here's a look at the trend and what it may mean for your own lab.

Continued on page 2

Brief Your CEO: Make Sure Lab Staff Know about New CMS Clarification of IDTF Billing Rules

If your lab or facility is an Independent Diagnostic Testing Facility (IDTF), you need to know and brief your C-Suite about the new Centers for Medicare & Medicaid Services (CMS) issued new guidance making some significant clarifications on billing, coding and coverage requirements. Here are seven things IDTF compliance managers should cover in their briefing.

Which Labs IDTF Billing Rules Affect

Before you begin you need to figure out if the new guidelines affect you. The answer is YES if your lab or facility is an

Continued on page 11

From the Bench: Courts Create New Defense for False Claims Based on Reasonable Mistakes about Regulatory Requirements, *from page 1*

What the FCA Says

As with many regulatory laws, FCA violations have two elements, both of which the prosecutor or whistleblower has the burden of proving:

- An action—submitting or causing a false claim for payment to be submitted to the government; and
- "Scienter," i.e., a state of mind that a defendant must have in committing the action—knowingly.

The FCA defines "knowingly" as "actual knowledge," "deliberate ignorance" or "reckless disregard." Historically, misunderstanding a confusing federal coverage or billing regulation has been interpreted as falling into the "reckless disregard" category. However, in a 2007 case called *Safeco Insurance Co. of Am. v. Burr*, 551 U.S. 47, the U.S. Supreme Court drew some lines by finding that misinterpretation may be a defense to the scienter requirement as long as:

- The defendant's interpretation was objectively reasonable; and
- "Authoritative guidance" didn't warn the defendant away from its interpretation.

In this case, the defendant's interpretation was reasonable and there was no guidance from the agency enforcing the law, the U.S. Federal Trade Commission, that "might have warned it away from the view it took."

The Safeco Standard Catches On

Technically, *Safeco* was an interpretation of the *Fair Credit Reporting Act* (FCRA), rather than the FCA; and the scienter standard under the FCRA is "willful," rather than "knowingly." However, the "reckless disregard" phrase that appears in the FCRA interpretation of "willful" is also used in the FCA definition of "knowingly." **Result:** The logic of *Safeco* would seem to apply equally to the FCA.

In fact, five different federal Circuit courts have extended *Safeco* to FCA claims. On Aug. 12, 2021, the Seventh Circuit joined the D.C., Third, Fifth and Eighth Circuits in this view.

The *Schutte v. SuperValu* Case

At issue were Medicare Part D regulations limiting drugs reimbursement to a pharmacy's "usual and customary" (U&C) costs. A pair of pharmacists filed a whistleblower lawsuit accusing the SuperValu grocery chain of knowingly submitting false claims by listing its pharmacies' retail cash prices—the price for uninsured cash customers—as its U&C price, rather than lower, price-matched amounts charged to qualifying customers under its discount program. The government decided not to intervene in the case.

LCA

Glenn S. Demby, Executive Editor

Barbara Manning Grimm, Managing Editor

Jim Pearmain, General Manager

Andrea Stowe, Business Development

Pete Stowe, Managing Partner

Mark T. Ziebarth, Publisher

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

The lower court agreed with the whistleblowers that SuperValu should have reported its lower, price-matched prices because that's what the definition of U&C price in the regulations required. But *Safeco* saved the day for SuperValu. The court ruled that the whistleblowers didn't prove that SuperValu submitted the false claims "knowingly" and partially dismissed the case.

The whistleblowers appealed, but to no avail. The standard the Supreme Court used to evaluate scienter under the FCRA applies equally to "knowingly" under the FCA, the Seventh Circuit affirmed. SuperValu's use of retail cash prices was a reasonable interpretation of the U&C rules, the Court reasoned, since they required pharmacies to use the prices they charge the "general public." And the discount rates the whistleblowers said SuperValu should have used weren't the ones it charged the general public.

The Court also concluded that there was no "authoritative guidance" that should have warned SuperValu away from its interpretation of U&C. On the contrary, the Centers for Medicare and Medicaid Services (CMS) didn't issue any guidance explaining the requirement; nor were there any circuit court rulings on the issue.

U.S. ex rel. Schutte v. SuperValu, No. 11-cv-3290 (7th Cir. Aug. 12, 2021)

Takeaway

FCA liability for knowingly submitting false claims is extremely broad. Until recently, there has been no cushion for labs that billed Medicare and other federal health programs based on a faulty interpretation of regulatory requirements. But Safeco and its progeny have the potential to blow the FCA liability scheme wide open. What especially keeps enforcers, whistleblowers and their attorneys up at night is that the "reasonable" standard is objective, rather than subjective. In other words, it doesn't matter if the lab actually believed that its misinterpretation of the regulatory requirement was or might have been wrong, as long as it can show that it's one that a reasonable third party would have made.

However, the second prong, or "authoritative guidance" of the Safeco test is also something labs must reckon with. Although no court has yet offered an official definition, it's clear that in interpreting regulatory requirements, labs and other providers must look not only at the regulations themselves but also guidance from CMS, OIG and other government agencies, as well as court rulings on and above the circuit court level.

Labs IN COURT

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

Fort Worth Hospital Settles Upcoding Charges for $3.3 Million

Case: A compliance officer morphed into a whistleblower when hospital leaders ignored her warnings about widespread billing and coding abuses. Specifically, she sounded the alarm that the hospital was improperly appending modifiers -25, -59 and -XU to secure improper payments. It wasn't just a small glitch. The modifiers were misused between 70 and 95 percent of the time, meaning the hospital was essentially double billing for these kinds of claims. While not admitting liability, John Peter Smith Hospital has chosen to settle the claims for $3.3 million, $912,635 of which will go to the whistleblower.

Significance: Modifiers -25, -59 and -XU indicate that a provider delivered significant care on the same day as another medical procedure performed on the same patient. The modifier signals that the care was above and beyond the preoperative and postoperative care "bundled" into the main procedure code and should thus be reimbursed separately. In addition to allegedly misusing the modifiers on hundreds of claims, the hospital failed to reimburse payors for the resulting overpayments it received.

Georgia Lab Shells Out $200K to Settle Genetic Testing Kickback Claims

Case: A psychiatrist brought a *qui tam* whistleblower lawsuit claiming that the consulting firm he worked for was taking kickbacks from Georgia genetic testing lab Alpha Genomix Laboratories in exchange for Medicare patient referrals of medically unnecessary tests that weren't actually ordered by physicians. According to the claim, the lab gave the firm illegal remuneration in the form of paying the salary of one of its employees. Rather than risk a trial, the lab will pay up to $200,000 to settle the case.

Significance: Genetic testing kickbacks and false have become a new favorite target for government enforcers and whistleblowers. One of the more interesting aspects of this case is the structure of the settlement, dictated by the fact that Alpha Genomix went bankrupt after the events of this case took place and was subsequently acquired by new ownership. The lab will pay $35,000 upfront and a percentage of gross annual company revenues of up to $200,000 later. The whistleblower is in line for 15 percent to 30 percent of whatever the government recovers.

Payor Can't Use Alleged Co-Conspirator's Settlement as Evidence Lab that Engaged in Pass-Through Billing Scheme

Case: Imagine this. Insurers sue you and other labs for conspiring with a hospital to commit a fraudulent pass-through billing scheme for lab tests. You think the case is garbage and are determined to wage a vigorous defense at trial. But the other labs aren't willing to risk a trial and decide to settle. **Question:** Can the insurer use the fact that the other labs settled as evidence? A Missouri federal court recently confronting this issue ruled no.

Significance: Federal rules of evidence ban the use of settlement offers, agreements and negotiations to "prove or disprove the validity" of a disputed claim at trial. The insurer cited an exception allowing information about a settlement that explains why a party has suddenly disappeared from a trial. But the labs in this case settled way before the case began and were never introduced to the jury. So, the exception didn't apply.

Rightchoice Managed Care, Inc. v. Hosp. Partners, Inc., 2021 U.S. Dist. LEXIS 177176

Federal Court Upholds $46.7 Million Medicare PHPs Fraud Conviction

Case: In 2015, the former president of a Texas hospital was ordered to pay restitution of $46,753,180 and spend 45 years in prison after being found guilty of 10 counts for his role in a $158 million Medicare Partial Hospitalization Programs (PHPs) fraud scheme. Now age 76, the president made a bid to get the convictions set aside but the Texas federal court said no dice and let the convictions stand.

Significance: The laundry list of defenses that the court rejected included, among others:

- Defense counsel was ineffective because it didn't research federal law on PHPs or object to certain evidence;
- The evidence supporting his convictions was insufficient;
- The prosecution's evidence gathering wasn't an illegal search and seizure under the Fourth Amendment;
- He wasn't denied his Fifth Amendment due process rights;
- The prosecution's failure to call a certain witness didn't deny him of his Sixth Amendment right to confront witnesses against him; and
- The government didn't commit entrapment.

United States v. Gibson, 2021 U.S. Dist. LEXIS 179712

TOOL MODEL CODE OF CONDUCT FOR VIRTUAL MEETINGS

Far from eliminating workplace harassment, telecommuting has only caused it to morph into digital forms. As a result, labs and other employers need to tweak their harassment policies to deal with the new face of harassment. The virtual meeting, in particular, has become the digital age version of the holiday office party where employees feel emboldened to do and say things they wouldn't dream of doing and saying to co-workers in-person. How do you crack down on this behavior? The starting point is to implement a Code of Conduct Virtual Meetings. Here's a template you can adapt.

Model Code of Conduct for Virtual Meetings

1. POLICY

XYZ Laboratories commitment to providing a work environment that is harassment-free, respectful and safe—both physically and psychologically—extends to all employees regardless of whether they work in XYZ facilities or virtually from a home office or other remote location. It is essential for employees to understand that the XYZ Laboratories Workplace Harassment Policy applies not just on XYZ premises but all locations where employees perform their work duties.

Workplace harassment will not be tolerated in any form or in any venue.

2. PURPOSE

The purpose of this Code of Conduct is to establish clear ground rules for behavior for virtual meetings so that all employees understand what is and is not acceptable during such meetings.

3. UNACCEPTABLE BEHAVIOUR

For purposes of this Code, unacceptable behavior includes:

- Harassment, intimidation, or discrimination in any form;
- Inappropriate comments, chat messages or verbal or other forms of abuse of any attendee, guest or other person, including but not limited to comments related to gender, sexual orientation, gender identity, disability, physical appearance, body size, race, religion, national origin, political belief or source of income;
- Yelling at, threatening or personally insulting any attendees, guests or other persons, whether verbally or physically;
- Inappropriate use of nudity and/or sexual images in public spaces or presentations;
- Stalking or directing unwanted sexual attention to any attendee, guest or other person; and
- Improper disruptions or outbursts.

4. OTHER RULES OF CONDUCT

During virtual meetings, all employees will be expected to respect common-sense rules for public behavior, personal interaction, courtesy, and respect for private property, and be considerate and respectful of differing perspectives during the meeting. In addition, employees must comply with the following rules during virtual meetings:

- Attire must meet the requirements for business dress set out in the XYZ Laboratories Dress Code;
- The recording or transmission of any meeting sessions or presentations is strictly prohibited unless the manager in charge or HR department directs or provides advance written consent of such recording or transmission;
- Smoking or vaping are not allowed during virtual meetings; and
- Microphones should be muted except when an employee is speaking.

5. REPORTING OF VIOLATIONS

Employees should immediately report any violations of this Code of Conduct that they experience or

witness to [*designated person/office*] using the forms, procedures and protocols for reporting harassment set forth in the XYZ Laboratories Workplace Harassment Policy. All such reports will be investigated following the investigation procedures contained in that Policy and employees will in no way be subjected to reprisal or retaliation for submitting such reports.

6. DISCIPLINE

Employees determined to be in violation of this Code of Conduct will be subject to discipline, up to and including termination, in accordance with the provisions of the XYZ Laboratories Progressive Discipline Policy and any applicable collective bargaining agreements.

Compliance Perspectives: How to Give Your Analog Workplace Harassment Policy a Digital Makeover

One of the only nice things about the pandemic is the relief it's provided from workplace harassment. After all, employees are far less vulnerable to workplace harassment when they work from home.

Right?

Absolutely wrong!!!

Since the pandemic began:

- More than 4 in 10 U.S. workers (41 percent) reported that they've been subjected to some form of digital harassment (Pew Research);
- Nearly half (45 percent) of women experiencing sexual harassment say it happened remotely (Rights of Women, UK and Wales ("ROW"));
- 23 percent of women reporting that they've been harassed say the problem has actually gotten worse since they began working from home (ROW); and
- More than 7 in 10 (73 percent) of victims say they don't think their employer is doing enough to protect them from remote harassment (ROW).

Same Problem, New Media

Far from eliminating harassment, the migration of employees to the home workplace has only caused it to go virtual. Cyberbullying, hate speech, stalking and other similarly nasty behaviors have thrived in pandemic conditions. Purveyors of harassment have also gotten better at using video conferencing, social media platforms, virtual discussion groups and other technologies to unleash new forms of harassment like zoom bombing, doxxing and dogpiling.

Continued on page 8

Compliance Perspectives: How to Give Your Analog Workplace Harassment Policy a Digital Makeover, *from page 7*

The Me Toobin Movement

The symbolic "coming out party" of digital harassment occurred last November when highly renowned magazine writer Jeffrey Toobin exposed his genitals to co-workers during a Zoom call. Toobin quickly apologized and claimed he didn't realize he was actually on camera. But the damage was done. After Toobin's suspension, Twitter users went online to share their own workplace harassment war stories under the #MeToobin hashtag.

Unfortunately, employers haven't adapted nearly as well. As employer, you're legally obligated under OSHA, discrimination and other laws to protect your employees from workplace harassment regardless of where they happen to work. But you can't prevent digital harassment with old-fashioned policies designed for analog threats. What's needed, and rather urgently, is for employers to review and, if necessary, revise their harassment policies to deal with the new face of harassment. Specifically, there are 5 ways your lab may need to broaden its current harassment policy to protect employees from digital threats.

1. Broaden Definition of "Harassment"

Pitfall: Standard policy definitions of "harassment" list forms and examples of prohibited conduct—name-calling, threats, stalking, etc. But the focus is typically on in-person behavior with no mention of online harassment. This critical policy omission may add to the false sense of security some employees experience when they're behind a computer screen and feel emboldened to make comments that they wouldn't dare utter to a co-worker in-person.

Solution: Make sure your policy definition covers common forms of online harassment that employees are likely to commit or experience, including:

- **Hate speech**, which you should define narrowly as including communication that attacks, discriminates or uses pejorative language to induce hatred, contempt or violence against a person or group on the basis of their race, colour, descent, sex, religion, ethnicity, etc.;
- **Cyberbullying**, or willful and repeated harm inflicted via computers, cell phones and other electronic devices;
- **Impersonation**, or posting harassing comments, photos or other materials in somebody else's name, typically in an attempt to get that person into trouble;
- **Swatting**, a dangerous (but thankfully, relatively rare) form of impersonation involving online threats designed to get a SWAT team to bust down the impersonated individual's door;

- **Hacking**, whether it's done to steal personal information, sabotage an IT network or simply harass somebody;
- **Denial-of-Service (DoS) attacks**, i.e., flooding a host or network until it crashes in a malicious attempt to prevent employees, customers and other legitimate users from accessing an organization's website;
- **Doxxing,** or collecting documents (docs) containing an individual's private information and posting them online for all the world to see and use;
- **Trolling**, or posting nasty and provocative things online in an attempt to upset, instigate and stir up trouble;
- **Dogpiling**, a form of trolling typically carried out by hundreds and even thousands of people seeking to overwhelm a website or social media page by posting negative comments on it at the same time; and
- **Message bombing**, which is similar to dogpiling that targets inboxes to make it impossible to respond to legitimate messages.

2. Broaden Definition of "Workplace"

Pitfall: One of the hallmarks of an obsolete harassment policy is its limitation to the organization's facility or at organization-sanctioned events. This is out of step with not only digital threats but also many state OSHA duties to prevent harassment in the "workplace," which is broadly defined to include any site where employees carry out their employment duties on the employer's behalf.

Solution: Make sure your policy definition of "workplace" covers all forms of carrying on business and all work-related settings where harassment can occur (including after-hours), including:

- Home work spaces;
- Client and customer visits and service calls;
- Business travel;
- Conferences, training sessions and seminars;
- Lab- or client-sponsored social functions;
- Other offsite work assignments.

Model Language

For purposes of this policy's ban on workplace harassment, "workplace" means anywhere where XYZ Laboratories employees are conducting business on Laboratories' behalf, including but not limited to, conducting business in person on Laboratories' facilities, premises or from a home or remote setting, on the phone, virtually, or through email or other social media and/or during after-hours events such as, but not limited to, business meetings, dinners, trainings, and during work-related travel.

Continued on page 10

Compliance Perspectives: How to Give Your Analog Workplace Harassment Policy a Digital Makeover, *from page 9*

3. Implement Code of Conduct for Remote Meetings

Pitfall: The virtual meeting has become the digital age version of the holiday office party where employees feel like the normal rules against acting like a pig don't apply. Regrettably, old school harassment policies are ill-suited to these venues.

Solution: Whether as part of your current harassment policy or in a separate policy, create and strictly implement a written code of conduct for remote meetings. Like the template on page 6 and the G2 website, make sure your code:

- Clearly states that your workplace harassment policy applies to remote work and virtual meetings;
- Specifically defines what conduct is unacceptable;
- Addresses the reporting and investigation of complaints; and
- Provides for discipline against those who commit violations.

4. Guard Against Digital Harassment from Third Parties

Pitfall: In a recent study, researchers reviewed the workplace harassment policies of 129 universities and colleges found that only 41 one of them acknowledged online harassment. They then analyzed those policies and found a common flaw: The policies were designed to protect employees and students against harassment committed by other people at the institution. The problem is that the employees and students who actually experienced online harassment reported that it usually came from people outside of or unknown to the institution.

Solution: Your commitment to protect employees from workplace harassment should cover harassment from all sources, not just other people at the lab or in your network, including patients, clients, vendors, contractors and their employees as well as unknown third parties.

5. Ensure Employees Can Report Harassment Remotely

Pitfall: Another potential disconnect to guard against is requiring employees to be present on the lab site to report the harassment they experience.

Solution: Make sure there's an online mechanism for telecommuters and other remote employees to report harassment to HR. Emphasize that you'll take all harassment complaints seriously and investigate them promptly, regardless of whether they're submitted in-person or online.

Brief Your CEO: Make Sure Lab Staff Know about New CMS Clarification of IDTF Billing Rules, *from page 1*

IDTF, i.e., a facility that's independent of both an attending or consulting physician's office and of a hospital. IDTFs may be either a fixed location or a mobile entity. Other than hospital-based and mobile IDTFs, a fixed-base IDTF doesn't:

- Share a practice location with another Medicare-enrolled individual or organization;
- Lease or sublease its operations or practice location to another Medicare-enrolled individual or organization; or
- Share diagnostic testing equipment used in the initial diagnostic test with another Medicare-enrolled individual or organization.

IDTF Billing Clarifications Your Briefing Should Cover

When an IDTF provides diagnostic procedures in a physician's office, IDTF general coverage and payment policy rules apply. Medicare reimburses diagnostic procedures performed by IDTFs at the Medicare Physician Fee Schedule (MPFS) rate. The IDTF billing clarifications are contained in the Medicare Learning Network (MLN) Booklet that CMS issued in September. There are seven points of clarification on which you should brief your lab executives:

1. Reimbursement of Nurse Practitioner Supervised Tests

Remind your audience, which should include at least one person from or who has knowledge of billing and coding requirements, that CMS has issued waivers on certain billing rules to make it easier for Medicare patients to access lab and other diagnostic tests during the COVID-19 Public Health Emergency (PHE), including allowing nurse practitioners, clinical nurse specialists, physician assistants and certified nurse-midwives to provide the required level of supervision for reimbursement under the MPFS.

2. Billing & Coding of Transtelephonic & Electronic Monitoring Services

Explain that the Booklet lists important coding clarification you need to cover in your briefing if your IDTF provides 24-hour EKG monitoring or other transtelephonic and electronic monitoring services without actually seeing a patient. Most, but not all of the current billing codes for these services are 93040, 93224, 93225, 93226, 93270 and 93271. CMS doesn't currently have specific certification standards for IDTF technicians.

If an entity lists and bills codes 93268, 93270, 93271, or 93272, the Booklet explains, the Medicare Administrative Contractor (MAC) must make a written determination that the entity has a person available on a 24-hour basis to answer telephone inquiries. Use of an answering service instead of the actual person isn't acceptable, the Booklet clarifies.

Continued on page 12

Brief Your CEO: Make Sure Lab Staff Know about New CMS Clarification of IDTF Billing Rules, from page 11

Billing Instruction: List the person performing the attended monitoring in Section D of Attachment 2 of Form CMS-855B

3. Global Billing

According to the Booklet, global billing is acceptable when the same entity performs both the TC and Modifier 26 and that entity provides both the TC and Modifier 26 within the same MPFS payment locality. It's okay to provide the TC and Modifier 26 in different locations, as long as you furnish them within the same MPFS payment locality.

Note: As with all services payable under the MPFS, CMS uses ZIP Code to determine the appropriate payment locality and corresponding fee used to price the service that's subject to the anti-markup payment limitation. When a ZIP Code crosses county lines, the agency uses the dominant locality to determine the corresponding fee.

Billing Instruction: If you bill with the global diagnostic test code, report the name, address, and National Provider Identifier (NPI) of the location where you provided the TC in Items 32 and 32a (or the 837P electronic claim equivalent).

4. Separate TC & PC Billing—Non-Global Billing

Billing Instruction: Let listeners know that when you bill the TC and Modifier 26 separately (not billed globally), you're supposed to report the name, address and NPI of the location where you performed each component. If the billing provider has an enrolled practice location at the address where the service took place, the billing provider or supplier may report their own name, address and NPI in Items 32 and 32a (or the 837P electronic claim equivalent).

The NPI in Item 32a must correspond to the entity identified in Item 32 (no matter if it's the group, hospital, IDTF, or individual physician), the Booklet explains. The only exception for Medicare claims is when a provider performs a service out of jurisdiction and is subject to the anti-markup or a reference lab service.

5. IDTFs & Opioid Treatment Programs (OTPs)

CMS clarifies that for an IDTF to be eligible to enroll as an OTP service provider with Medicare, its program must have current, valid, and full certification by the Substance Abuse and Mental Health Services Administration (SAMHSA), and meet all of SAMHSA's criteria, including but not limited to:

- Drug Enforcement Administration (DEA) registration;
- State licensure; and
- Accreditation.

6. Coverage of SNF Residents Requiring Transportation for IDTF Service

Explain that in 2018, CMS revised both the Medicare Benefit Policy Manual and Medicare Claims Processing Manual to clarify that Part B may cover a medically necessary ambulance transport from an SNF to the nearest supplier of medically necessary services not available at the SNF where the patient is the resident, including the return trip (including an IDTF). Tell your listener that CMS has now clarified that this rule applies to patients in an SNF stay uncovered by Part A, but who have Part B benefits.

For SNF residents receiving Part A benefits, such ambulance trips to IDTFs for medically necessary services are subject to SNF consolidated billing.

7. Billing of IDTF Mammography Services

Again, set the context by explaining that under (Chapter 18, Section 20.3.1.4 of) the Medicare Claims Processing Manual, if an IDTF furnishes any type of mammography service (screening or diagnostic), it must have an FDA certification to perform such services. However, if you only perform diagnostic mammography services, you shouldn't enroll as an IDTF. Medicare does pay for screening mammographies (including those that are self-referred) when an IDTF performs them at the IDTF facility.