G2 INTELLIGENCE
A DIVISION OF PLAIN LANGUAGE MEDIA

G2 Compliance Advisor

For Clinical and AP Laboratories and Pathology Practices

August 2015

Inside this issue

www.G2Intelligence.com

Court Decides "Absurd" Is Worse Than "Potentially Unworkable" When Interpreting 60-Day Repayment Rule

A federal district court has weighed in on the meaning of "identified" for purposes of determining when Medicare and Medicaid overpayments must be returned to avoid violating the False Claims Act (FCA). In *Kane v. Healthfirst, Inc.* and *U.S. v. Continuum Health Partners, Inc.*, a New York federal court resolved the debate about when the Affordable Care Act's 60-day deadline for returning overpayments begins to run, explaining the deadline is triggered when providers are on notice that they may have received overpayments—not after they've determined with certainty the precise amount.

Continued on page 9

LabMD Trial Held; Company Continues to Fight

The saga of LabMD v. the Federal Trade Commission (FTC) continues to twist and turn as more information comes to light about the business practices of "cyber intelligence" company Tiversa, Inc. and the FTC's heavy reliance on Tiversa's claim that LabMD failed to secure patients' data.

It's now been two years since the FTC first launched its investigation and filed a complaint against the Atlanta-based medical testing firm for an alleged data security breach which the FTC claimed violated section 5 of the FTC Act, which prohibits fraudulent, deceptive and unfair business practices. The investigation was based on a LabMD health insurance computer file that contained patient protected health information (PHI) on more than 9,000 people (the "1718" file) that had allegedly been exposed on the Internet. Tiversa informed LabMD that it found the 1718 file on a peer-to-peer file sharing network, and notified the FTC about the security breach after LabMD refused to contract with Tiversa for security monitoring services.

After months of delay, the evidentiary hearing in the case before presiding FTC administrative law judge D. Michael Chappell was completed July 15 and the record closed July 20.

Some of the most explosive testimony came from key witness Richard Wallace, a former Tiversa employee turned whistleblower, who was granted immunity to appear (*see G2 Compliance Advisor January 2015*). He testified May 5 that, among other things, Tiversa manufac-

Continued on page 2

LabMD Trial Held; Company Continues to Fight, *from page 1*

tured evidence using phony IP addresses to make the 1718 file look like it had been downloaded by several known identity thieves when in actuality he downloaded the 1718 file from LabMD's own server; he made the data breach look worse than what it was at the direction of Tiversa's CEO Robert Boback when LabMD refused to enter a monitoring contract with Tiversa; Tiversa has deceived many businesses this way to get them to contract with the company; and that Tiversa provided false information to the FTC.

LabMD is also now claiming that the proceedings violate the U.S. Constitution because the presiding administrative law judge was not appropriately appointed.

Tiversa has defended itself, saying that Wallace's allegations were "baseless" and coming from a "terminated employee."

Several days after Wallace's testimony, Congressman Darrell Issa released the staff report from the House Oversight and Government Reform Committee, prepared in February but embargoed until Wallace testified. The report found, among other things, that:

- Tiversa was no "white knight" but instead often acted unethically and sometimes unlawfully in its use of documents unintentionally exposed on peer-to-peer networks
- Tiversa CEO Boback and at least one employee under his direction provided false information to the U.S. government
- Tiversa obtained non-public advance knowledge of FTC enforcement actions from which it attempted to profit
- Tiversa used "unseemly" business practices such as fearmongering and mining files for "potential" clients
- Tiversa provided information on LabMD and almost 100 other companies to the FTC when they refused to do business with Tiversa
- The FTC and Tiversa misrepresented their relationship, and the FTC failed to question the information Tiversa provided or Tiversa's creation of a "dubious" shell organization to funnel information to the FTC
- Tiversa withheld documents from the FTC.

In light of all of this information, LabMD filed a motion June 19 with the FTC requesting that the Department of Justice investigate Tiversa and Boback for potential criminal activity, including perjury, knowingly obtaining or disclosing individually identifiable health information maintained by LabMD without authorization or for commercial gain, conspiracy, computer crimes, obstruction and falsification of records.

The FTC did not join in this motion but didn't oppose it, either. Tiversa and Boback have asked the FTC for time to file a response to this motion, calling the accusations "serious yet baseless" and designed to impugn their reputations.

LabMD, whose attempts to dismiss the FTC's complaint have been denied, filed an Answer and Defenses July 31. It again denies that it violated section 5 of the FTC Act, and claims that the FTC didn't have the authority to regulate the acts alleged in the Complaint against LabMD. Even if it did have such authority, because the FTC has issued no rules, regulations or guidelines for businesses to follow in order to comply with the Act, LabMD asserts the FTC complaint against it violates LabMD's due process rights.

LabMD is also now claiming that the proceedings violate the U.S. Constitution because the presiding administrative law judge was not appropriately appointed.

The FTC's proposed order would require LabMD to institute compensative data security measures and be evaluated by the agency every two years for 20 years. (*See G2 Compliance Advisor October 2013*). LabMD has stated that it has been forced to cease operations due to the FTC's actions against it.

The last deadline for post trial briefs is September 4.

The underlying importance of this case is whether and to what extent the FTC has authority to investigate and impose enforcement actions for data breaches.

Case may have long term consequences

The underlying importance of this case is whether and to what extent the FTC has authority to investigate and impose enforcement actions for data breaches. LabMD has repeatedly asserted that since as a covered entity it is subject to HIPAA, any data breach it may have suffered should be investigated not by the FTC but by the Department of Health and Human Services' Office for Civil Rights (OCR), which enforces that law and which has published numerous regulations and guidance to help organizations comply with it.

The FTC and OCR appear to take different approaches to data security breach enforcement. The FTC prefers to impose long term corrective action plans, such as the one proposed for LabMD. In contrast, OCR prefers to resolve HIPAA violations more informally and with education. It has issued more formal, punitive settlements only in 26 situations where it found multiple HIPAA violations and wants to set an example regarding particular conduct. For instance, its latest Resolution Agreement, announced in July, fines a hospital $218,400 for exposing patient files by using an unauthorized, unsecure Internet-based document sharing application to store documents, but the accompanying evaluation by OCR is only for one year.

The FTC also differs from the OCR in that it deals only with companies in interstate commerce, but is concerned with all consumer information, not just patient PHI.

If the FTC prevails in the LabMD case, it will likely continue or even ramp up its enforcement of data breaches, even in the absence of extensive rules regarding what it expects of businesses. It did offer an explanation in a May 20 blog post about its process when it investigates a data security breach. It also issued a new security guide in July aimed to helping businesses keep data secure. The tool provides 10 "practical lessons" pulled from various enforcement actions the FTC has taken involving security breaches. Each lesson uses a specific FTC settlement as an example, although none of them involve health care entities. Many of the tips are similar to those found for HIPAA compliance and are rather basic, such as requiring complex passwords. It is not yet known whether these offerings provide sufficient guidance to companies in FTC's crosshairs.

However, the new information about Tiversa calls into serious question the FTC's reliance on Tiversa in its investigation of LabMD, which could affect the outcome of this case and the agency's enforcement efforts in the future. The bottom line, of course, is that apparently LabMD did have some problems with data security if the 1718 file could end up in Tiversa's hands.

Takeaway: Compliance officers should be aware that labs currently can be investigated by both OCR and the FTC in the event of a security breach. Steps should be taken to comply with both HIPAA and the FTC Act and use due diligence to keep consumer information safe. G2

AMP Offers Proposal for Regulation of Laboratory-Developed Tests

Last month in Compliance Perspectives, we highlighted the current status of the Food and Drug Administration's proposed regulation of laboratory-developed tests (LDTs). While the FDA's proposed framework remains to be finalized, other stakeholders are proposing alternative oversight models. This month, the Association for Molecular Pathology issued a proposal for modernizing CLIA regulations. The proposal reiterates AMP's position that FDA regulations are not appropriate for professional services and refers to the testing as laboratory developed testing procedures or LDPs. Representatives from AMP presented the recommendations to the Senate Health, Education, Labor, and Pensions (HELP) Committee, which is now drafting legislation that would provide opportunities for enhanced support for medical innovation and patient access to new medicines and technologies. The proposal's stated objectives include ensuring "[r]egulatory oversight does not slow innovation, constrain flexibility and adaptability, or limit a test's sustainability as a result of being unduly burdensome and beyond the fiscal capacity for the laboratory to reasonably perform or the health care system to financially support."

Explaining the need to update the CLIA regulations, the proposal highlights the growth and evolution of molecular diagnostics and distinguishes LDPs from medical devices asserting that one set of regulations "can never address both adequately."

Identifying specific sections of the CLIA regulations for updating, the proposal describes a tiered, risk-based model. The review process for each risk category is as follows:

- **Low-risk:** validated by the laboratory, put into service, and subject to inspection in the normal course of laboratory inspection.
- **Moderate-risk:** information submitted for third party review at least 30 days before the test is offered to the public with a time limit on the review process and grandfathering provision for previously introduced LDPs.
- **High-risk:** information submitted for third party review at least 90 days before the test is offered to the public, with a time limit on the review process.

Multianalyte assays with algorithmic analyses (MAAAs) with proprietary algorithms would be submitted to FDA unless the laboratory reveals its proprietary algorithm to third party review and inspection.

The proposal also includes publication requirements geared to providing transparency for providers, patients and regulatory agencies, and allowing comparisons between LDPs by giving access to information about "accuracy, precision, and known clinical significance of an LDP." Addressing concerns raised by many in the debate about FDA regulation in this area, the proposal also: 1) calls for development of a minimum level of standards and time frames for submitting information about a new laboratory developed procedure prior to offering the test to the public and imposes presumptive approval if the reviewing party doesn't make a determination in the required time period; 2) addresses types of evidence for demonstrating clinical validity; and 3) discusses when modifications to an LDP or to an FDA cleared or approved IVD require notice or a new review. Finally, to fund the oversight functions, the proposal allows for an annual fee linked to a laboratory's number of LDPs and "limited to cost recovery."

Takeaway: The debate concerning oversight of laboratory developed testing continues with detailed alternatives to the FDA framework being recommended to legislators. G2

Compliance is About More than Kickbacks, Referrals, & False Claims Liability: Check Our Top 3 Compliance Areas You May be Overlooking

Violations of Medicare-related laws such as the Anti-Kickback Statute, self-referral law and the False Claims Act can cost laboratories and pathology groups potentially millions of dollars and thus, compliance regarding these laws gets a lot of attention. However, there are other compliance risks laboratory compliance officers shouldn't lose sight of as well.

While the OIG, DOJ, CMS, and FDA may be acronyms that you think of most often when you think of compliance, there are some other enforcement agencies that should also figure prominently in compliance programs. In this article we'll focus on three government agencies that should be getting your attention:

OSHA's bloodborne pathogen standards require regular training for workers before they work with blood and the training must address what to do in response to an exposure incident.

#1. OSHA

As employers, laboratories have a duty to provide a safe workplace for their employees. The Occupational Safety and Health Administration (OSHA) enforces workplace safety law which includes a general duty clause that covers a lot of ground. But there are some specific safety issues that labs should be paying particular attention to:

Bloodborne pathogens

Bloodborne pathogens are an obvious issue for clinical laboratories but it's often easy to overlook the obvious. Just about two years ago LabCorp found itself in trouble with OSHA and paid more than $50,000 in fines relating to bloodborne pathogen hazards. OSHA claimed that phlebotomy technicians didn't receive required training before working with blood and workers didn't receive training about handling exposure incidents.

More recently, this month, OSHA announced that an emergency medical transport company could be subject to more than $235,000 in fines after OSHA inspectors found during a February 2015 inspection that the company failed to protect workers from bloodborne pathogens. Allegations included claims that the company failed to train workers regarding hazards and precautions to prevent exposure and didn't require workers to use gloves and face masks when in contact with infectious materials.

OSHA's bloodborne pathogen standards require regular training for workers before they work with blood and the training must address what to do in response to an exposure incident. So do a compliance review of your training programs, and your policies and procedures with regard to bloodborne pathogens and make sure they are up-to-date and being consistently followed.

Workplace violence

Earlier this year, in an April 2015 press release, OSHA announced updated guidance for protecting healthcare workers from workplace violence titled *Guidelines for Preventing Workplace Violence for Healthcare and Social Service Workers*. In the press release, OSHA cited 2013 Bureau of Labor Statistics information that indicate more than 23,000 injuries occurred at work due to assault and "[m]ore than 70 percent of these assaults were in health care and social service settings." OSHA declared "health care and social service workers are almost four times as likely to be injured as a result of violence than the average private sector worker."

The updated guidance addresses research regarding the workplace violence causes and risk factors unique to health care work environments. The guidance also calls for written workplace violence prevention programs that include worker and management collaboration, analyzing the worksite, training, recordkeeping, and hazard prevention and control.

OSHA also requires that by June 2016 employers "update alternative workplace labeling and hazard communication program as necessary" and "provide additional employee training for newly identified physical or health hazards."

Hazard communication

In an effort to harmonize standards internationally, OSHA's Hazard Communication Standard was revised to now require chemical manufacturers and importers provide required hazard information on labels and material safety data sheets according to a specific set of harmonized criteria for classifying chemicals according to health and physical hazards.

Why is this important for laboratories if the manufacturers and importers must create compliant labeling? Because laboratories, like all other affected employers, are required to provide training to workers regarding this new communication standard. The safety data sheets include 16 specific sections and the new labeling requirements call for use of signal words, pictograms, a hazard statement, and precautionary statement. Initial training on these new labels and data sheets, to ensure workers understand the new formats and information provided, should already have been provided by the end of 2013. But the lab's obligations don't end there.

OSHA also requires that by June 2016 employers "update alternative workplace labeling and hazard communication program as necessary" and "provide additional employee training for newly identified physical or health hazards." Additionally, while the manufacturers have to supply the safety data sheets, your lab should conduct an inventory and make sure you've received all the updated safety data sheets that you need for your laboratory. Also, include this OSHA training as an item in your compliance audits to ensure all requirements are met and training is up-to-date. Just last month, July 20, 2015, OSHA announced instructions to compliance officers for how to ensure enforcement of the new Hazard Communication Standard.

On a related note, OSHA also currently is awaiting responses to a Request for Information on Chemical Management and Permissible Exposure limits. It extended the comment period until October 8, 2015. The initial request and specific questions on this topic was published October 10, 2014.

TB in health care settings

In July, OSHA issued updated instructions regarding inspections and enforcement concerning tuberculosis exposure in health care settings. While this doesn't change any employer obligations, it is a sign that OSHA is paying attention to this issue. The press release announcing the updated instructions highlights the fact that the new instructions cover "additional workplaces regarded as healthcare settings such as sites where emergency medical services are provided and laboratories handling clinical specimens that may contain M. tuberculosis."

Emphasizing the importance, OSHA notes that "[m]ulti-drug-resistant and extremely drug-resistant TB continue to pose serious threats to workers in healthcare settings." It also cites CDC statistics indicating that TB is "the second most common cause of death from infectious disease in the world" behind HIV/AIDS.

So your laboratory should review its policies and procedures and its TB infection control plan and make sure they are up to date and consistently implemented to reduce the risk of tuberculosis infection for your workers. The instructions state that TB infection control plans should be updated annually and supervised by appropriate personnel.

Injury reporting

Earlier this year the reporting rules changed. While laboratories have a partial exemption, some aspects have changed that affect all employers subject to OSHA—laboratories should be notifying within eight hours of fatalities or an employee being hospitalized, suffering amputation or eye loss. The amputation and eye loss reporting requirement is new and reports were only required when at least three employees were hospitalized rather than just one employee. Check to make sure your reporting procedures have been updated and that all employees are trained on these requirements.

The bottom line for laboratories is that with all these fairly recent developments in workplace safety, it's clear that OSHA hasn't gotten complacent and is updating its standards to respond to changing workplace environments and developing hazards. Thus laboratories must be vigilant and review safety policies and procedures to ensure laboratory workers are protected—or risk significant financial liabilities.

#2. IRS and DOL

For flexible staffing and filling in holes in your schedule, it may be appealing to hire independent contractors. But make sure your arrangement is truly an independent contractor arrangement and not employment. Just the label you give it isn't the determining factor.

The IRS looks at the degree of control and independence in three areas: behavioral control (regarding what the worker does and how he does it), financial control (the business aspects such as how the worker is paid and how expenses are handled) and type of relationship (is the arrangement written, does the worker get certain benefits such as pension, is the work performed a key aspect of the business?).

Whether a worker is an employee or independent contractor is important not just for tax considerations but also because employees are entitled to protection under the Fair Labor Standards Act.

Whether a worker is an employee or independent contractor is important not just for tax considerations but also because employees are entitled to protection under the Fair Labor Standards Act (regarding minimum wage, overtime, workers' compensation). So, in addition to the IRS, the Department of Labor (DOL) is also concerned about how workplaces classify their workers.

Finally, improperly classifying individuals as independent contractors could impact compliance with the Affordable Care Act (ACA) and obligations to provide health insurance benefits because an organization's number of employees affects its obligations under the ACA.

In July, the DOL issued an Administrator's Interpretation regarding the Fair Labor Standards Act's terms for classifying workers as employees and notes that its Wage and Hour Division has received "numerous complaints" from workers alleging misclassification as independent contractors and that in response to this "problematic trend" many states have established task forces focused on misclassification of workers. The DOL's July interpreta-

tion document also notes the agency has entered into a memorandum of understanding with the IRS and individual states to coordinate their efforts on this issue. In fact, memoranda were announced just this month between the DOL and the states of Alaska and Idaho.

Where to find more information

About Safety:

- You can find more information about the Occupational Health and Safety Act's general duty clause and its standards addressing specific safety issues at www.osha.gov
- The *Guidelines for Preventing Workplace Violence for Healthcare and Social Service Workers* is available at https://www.osha.gov/Publications/osha3148.pdf
- A Fact Sheet regarding the Hazard Communication Standard Final Rule is available at: https://www.osha.gov/dsg/hazcom/HCS-Factsheet.html
- The Centers for Disease Control and Prevention also provide information about workplace safety in the healthcare setting at www.cdc.gov/niosh/topics/healthcare/

About Worker Classifications:

- For information about classification of workers as employees or independent contractors, see both the Internal Revenue Service and Department of Labor, Wage and Hour Division.
- The IRS offers videos, publications, forms and other guidance to help understand this issue at www.irs.gov/Businesses. The IRS also provides a brief Tax Topics titled "Independent Contractor vs. Employee" that offers a concise, clear discussion of the applicable standards for classification.
- The Department of Labor's website provides news, guidance and information about its enforcement initiative at http://www.dol.gov/whd/workers/misclassification/

About Discrimination:

- For information about employment discrimination, see the Equal Employment Opportunity Commission's website at www.eeoc.gov. Guidance documents organized by topic are available at: http://www.eeoc.gov/laws/guidance/subject.cfm

The DOL indicates that in 2014, its Wage and Hour Division recovered a total of $79 million in back wages for more than 109,000 workers. While this has been getting a lot of attention in the home health industry, it's unwise for any employer, in any industry, to ignore the classification issue. If you are wrong in classifying workers as employees or independent contractors, you risk liability for unpaid income and unemployment tax withholdings, unpaid wages, unpaid workers' compensation premiums and other benefits and potential liability for failure to provide health insurance benefits under the ACA.

#3. EEOC

The Equal Employment Opportunity Commission (EEOC) may not be on your radar but as you struggle to adapt to a changing and competitive laboratory market and manage tight budgets, make sure your employment decisions don't give rise to claims of discrimination. Recently, in June, the EEOC called attention to pregnancy discrimination, issuing a Notice of Enforcement Guidance on the topic and recent enforcement cases have involved pregnancy discrimination.

Also, in July, a health care system agreed to pay $80,000 to settle disability discrimination claims. While that number is small potatoes compared to the numbers we see in False Claims Act enforcement, that settlement addressed claims involving just one individual.

Recent discrimination enforcement efforts have addressed pregnancy, disability, race and even genetic discrimination (an issue likely to become more important as the prevalence of genetic testing grows). So your compliance efforts should also include review of employment-related discrimination policies and procedures.

Court Decides "Absurd" Is Worse Than "Potentially Unworkable", *from page 1*

The federal and New York governments intervened in a whistleblower lawsuit, arguing the provider violated the FCA by "intentionally or recklessly" failing to timely repay overpayments. According to the court's discussion of the alleged facts, a health insurance company's "software glitch" had caused multiple hospitals in the same health system to submit improper Medicaid claims. Robert Kane, a health system employee assigned to investigate, produced a list of 900 potential overpayments but indicated further analysis was required to confirm which were improperly paid. Four days later, the employee was fired. While a few overpayments were returned shortly after that list was provided, the health system didn't repay hundreds of overpayments until two years after receiving the list and after the government filed a Civil Investigative Demand inquiring about the potential overpayments. The health system asked the court to dismiss the lawsuit arguing that the employee's list was only notice of *potentially* improper claims. Because further investigation was needed, the health system argued the list didn't "identify" overpayments triggering the 60-day deadline. The court disagreed.

> ***"[W]hile the Government's interpretation would impose a stringent—and, in certain cases, potentially unworkable—burden on providers, Defendants' interpretation would produce absurd results."***
>
> **—U.S. District Court Southern District of New York, *Kane v. Healthfirst, Inc.***

While the ruling isn't what providers would have liked to hear, there is some bit of good news to cushion the blow.

Bad news: Providers, not government, bear burden on repayment

The court explained that triggering the 60-day deadline only after providers did all they needed to "determine conclusively the precise amount owed to the Government" created "a perverse incentive to delay learning the amount due and relegat[ed] the sixty-day period to merely the time within which they would have to cut the check."

Health care attorney Robert E. Mazer of Ober Kaler in Maryland explains there are two issues—when an overpayment was identified and whether the failure to report and return the overpayment violated the FCA. In interpreting the statutory language regarding the identification of an overpayment, he says the court was "really very harsh and very strict."

The court looked to legislative history to interpret the meaning of "identified" and said that the FCA's knowledge standard included recklessness and deliberate ignorance and "Congress intended for FCA liability to attach in circumstances where, as here, there is an established duty to pay money to the government, even if the precise amount due has yet to be determined." To accept the defendant's argument that claims aren't identified until they are certain as to amount, "would make it all but impossible" to enforce that deadline in healthcare fraud cases, the court said. It decided that Congress expected providers rather than the government to bear the burden of quickly addressing and returning overpayments.

"[W]hile the Government's interpretation would impose a stringent—and, in certain cases, potentially unworkable—burden on providers, Defendants' interpretation would produce absurd results," the court decided.

The court considered CMS' interpretations of the term "identified" in two previous rules, finding its ruling "was at least consistent" with those interpretations. In 2012, CMS said an overpayment was identified when a provider "has actual knowledge of the overpayment or acts in reckless disregard or deliberate ignorance of the overpayment" and in a 2014 rule it said overpayments are identified "when the [entity] has deter-

mined, or should have determined through the exercise of reasonable diligence that [it] has received an overpayment." CMS also said that providers had an obligation to "make a reasonable inquiry" with "all deliberate speed" to determine if an overpayment exists.

Mazer notes that the defendants "made it a little bit easier for the judge" with a two-year delay and repayment occurring after the government's CID.

Good news: Good intentions and reasonable haste could avoid liability

But it's not all bad news, advises Mazer. While it would have been better if the court said "an overpayment is not 'identified' until known with certainty and quantified," the court's ruling referenced prosecutorial discretion and suggested that the government may not prevail on its FCA claim if it pursued a provider who was trying hard to return the overpayment but was beyond the 60 days, he explains. The court specifically acknowledged that investigating large numbers of claims within a 60-day timeline could be difficult and said prosecutors should "avoid enforcement actions aimed at well-intentioned healthcare providers working with reasonable haste to address erroneous overpayments." Thus, Mazer indicates the court "may look at whether [a provider] acted with reasonable diligence, which is a somewhat subjective standard, in determining whether an obligation is knowingly concealed or knowingly and improperly avoided or decreased in violation of the FCA."

Mazer notes that the defendants "made it a little bit easier for the judge" with a two-year delay and repayment occurring after the government's CID. "It would have been easier to swallow if it had been 65 days instead of 2 years and after a CID," Mazer says of the health system's delay. In fact, the court specifically called attention to the timing of repayment after the CID. It also noted the health system fired the worker four days after he provided the list of potential overpayments and supplied no evidence demonstrating it assigned anyone else to continue investigating the list. Additionally, the health system didn't provide its employee's analysis to the New York State Comptroller who inquired about the overpayments. All these facts undercut any argument the providers were acting diligent and waiting to determine which claims were in fact overpaid.

Finally, it's important to note that this ruling answered the defendant health system's request that the court dismiss the lawsuit before trial. The court refused to dismiss the lawsuit so this is not the final ruling in the matter. It means the defendant hasn't successfully argued that the government has no valid claim. In making such a decision, a court has to accept all the factual allegations made in the complaint as if they are true and make reasonable inferences in favor of the government plaintiffs, explains Mazer. To keep its claim alive and defeat such a motion, the government plaintiff has to show its claims are plausible—that there are enough facts to support more than a mere possibility the defendant violated the law. The court noted this in stating that "at a later stage in the proceedings" the defendants would have the opportunity to show they did investigate the potential overpayments but, so far, the government had sufficiently shown the health system "avoided returning the overpayments."

3 lessons learned

The good news is that the delay in this case was two years, clearly beyond the 60 days and this decision was just one court's interpretation, in response to a motion to dismiss. "But it's the only decision out there," points out Mazer. And, the stakes are high. Both the federal and New York governments are seeking treble damages from the health system in this case plus penalties in the amount of $11,000 for each overpayment under federal law and $12,000 for each overpayment under New York law. The final tally in these types of cases could be quite significant. In fact, Mazer notes the Department of

Justice recently announced a settlement agreement with a pediatric practice resolving false claims allegations including failure to timely return overpayments. That practice agreed to pay $6.8 million and enter into a corporate integrity agreement as part of the settlement. So consider the lessons learned from this case:

#1 Act diligently and speedily.
Mazer says his advice is unchanged by this ruling: If you have notice of a potential overpayment "work on it diligently, try to return it within 60 days. Even if you don't meet the 60 days, work with reasonable haste to confirm and quantify and return the overpayment." "It's hard to say what is reasonable haste—a term used by the court—," he adds, but it's "certainly doing something intended to bring disclosure in reasonable time."

This is one aspect that laboratories may have an advantage over other providers. "In the clinical laboratory setting it may well be that you have hundreds of claims that are virtually the same and don't require detailed analysis to determine if it's overpaid," says Mazer. Although this won't always be the case, when it is, you should be able to address the issue more quickly.

#2 Consider an interim report.
"Where it's clear that some amount of overpayment has been received, it's probably a good idea even if you can't complete everything you need to do within the 60 days, to report to the government that you have an overpayment issue, are reviewing it and … trying to determine the amount and repay it," says Mazer. Show the government what you are doing to try and comply. "It's an indicator of good faith." Note that the court highlighted in its ruling the fact that the health system didn't share its list of potentially overpaid claims with the New York Comptroller.

#3 Properly respond to employee reports of potential payment issues.
Pay attention when employees raise potential overpayment issues and respond appropriately. In this case, the government claims the health system fired the employee who gave notice of the potential overpayments and then did nothing to pursue an investigation. Mazer points out this could have all happened differently if the health system had repaid the overpayments relatively shortly after receiving Mr. Kane's list, even if not within the 60 days.

(*Kane v. Healthfirst, Inc.* and *U.S. v. Continuum Health Partners, Inc.*, No. 11 Civ. 2325(ER), S.D.N.Y. Aug. 3, 2015)

Takeaway: Federal court defines identified overpayments stringently but also raises potential for leniency for providers acting with "reasonable haste" to report and return overpayments.

G2 Compliance Corner

Don't Forget to Check Excluded Status

Background checks aren't just for spotting criminal records. Are you checking the Office of Inspector General's List of Excluded Individuals and Entities (LEIE)? In 2013, the Office of Inspector General issued a Special Advisory Bulletin highlighting the issue. No federal health care program payment can be made for any item or service that is furnished by an excluded person or at the medical direction or prescription of an excluded person. Excluded individuals also can't serve in an executive or leadership role or provide management services such as HIT, billing and accounting, or staff training for a provider that bills federal health care programs. Most relevant for laboratories is the prohibition on payment for items or services "furnished at the medical direction or on the prescription of an excluded person."

The OIG's Bulletin advised: "Many providers that furnish items and services on the basis of orders or prescriptions, such as laboratories, imaging centers, durable medical equipment suppliers, and pharmacies, have asked whether they could be subject to liability if they furnish items or services to a Federal program beneficiary on the basis of an order or a prescription that was written by an excluded physician. Payment for such items or services is prohibited. To avoid liability, providers should ensure, at the point of service, that the ordering or prescribing physician is not excluded."

Providers can face civil monetary penalties for billing for services linked to an excluded person—up to $10,000 for each item or service furnished by the excluded person and billed to a federal program. In March 2015, a health care system serving parts of Indiana and Ohio agreed to pay more than $120,000 to settle allegations it employed a laboratory technician who was an excluded individual and provided items and services to patients that were billed to federal health care programs.

To check excluded status of individuals, laboratories can use the OIG's LEIE online searchable database available on its website, oig.hhs.gov, under the tab Exclusions.

News at a Glance

USPTO Updates Interim Guidance for Patents Based On Natural Phenomena. The United States Patent and Trademark Office (USPTO) has updated interim guidance regarding the interpretation of patents based on natural phenomena. The guidance stems from significant U.S. Supreme Court rulings issued in 2012 and 2013 regarding patent battles over laboratory tests. Three years ago, the high court ruled in favor of the Rochester, Minn.-based Mayo Clinic in a patent dispute with Prometheus Laboratories over an esoteric blood test. Prometheus had claimed that the observation of natural phenomena—such as the results of the test—could be patented; but the court disagreed. Similarly, the Court ruled that a patent Myriad Genetics held on BRCA testing was invalid, concluding that a single human gene could not be protected under patent law. The update responds to more than 60 public comments received concerning initial interim patent eligibility guidance issued in 2014. Those comments address six themes including a request for additional examples addressing abstract ideas and laws of nature, how examiners identify abstract ideas, and an explanation of "the markedly different characteristics analysis." Public comments on this update must be submitted by October 28, 2015.

Drop in Senior Medicare Patrol Related Fraud Recoveries. The Senior Medicare Patrol (SMP) has been an initiative of the Centers for Medicare & Medicaid Services since the late 1990s, initially as a pilot project, and now operates initiatives in every state and territory, staffed by more than 5,000 volunteers. However, the SMP has had modest results in recent years, according to a new report from the Office of the Inspector General (OIG) for the U.S. Department of Health and Human Services. In calendar 2014, recoveries from Medicare and Medicaid fraud inquiries led to expected recoveries of ill-gotten payments totaling $661,333—a 93 percent decrease from 2013. But in 2013, much of the $9.1 million of expected recoveries were tied to what the agency called "a single event." The OIG also noted that "we continue to emphasize that the projects may not be receiving full credit for savings attributable to their work. It is not always possible to track referrals to Medicare contractors or law enforcement from beneficiaries who have learned to detect fraud, waste, and abuse from the projects. In addition, the projects are unable to track the substantial savings derived from a sentinel effect whereby fraud and errors are reduced by Medicare beneficiaries' scrutiny of their bills."

Laboratory Data and Interoperability to be Focus of FDA Workshop. Recognizing that laboratory tests "influence between 70 to 80 percent of clinical decisions," the Food and Drug Administration, Centers for Disease Control and Prevention (CDC) and the National Library of Medicine (of the National Institutes of Health) are holding a public workshop Sept. 28, 2015, to improve ease of sharing laboratory data. The agencies seek public input on "promoting semantic interoperability of laboratory data between in vitro diagnostic devices and database systems." Also at issue are the standards for reporting laboratory data and models for interoperability. The FDA indicated a discussion paper with more detailed discussion of the workshop's subject matter will be released online. A webcast of the workshop will also be available. Attendees must register by Sept. 18, 2015. Public comments are due by October 26, 2015. More information can be found in the FDA Notice published in the Aug. 3, 2015 Federal Register. G2

Kelly A. Briganti, JD, Editorial Director, Kelly@plainlanguagemedia.com; Barbara Manning Grimm, Managing Editor; 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.