LABORATORY ECONOMICS Volume 1, No. 5, July 2023

Kimberly Scott, Editor, kscott@laboratoryeconomics.com

COMPLIANCE & POLICY REPORT

Compliance and Regulatory Analysis for Lab Directors and Managers

FDA Preparing to Issue Proposed Rule on LDT Oversight

The Food and Drug Administration is preparing to publish in August a proposed rule making it explicit that it has authority to oversee laboratory-developed tests. The agency published a notice of proposed rulemaking June 14. *Continued on p. 8.*

Key Legal Hotspots for Laboratory Sales Reps: Tips on What NOT to Do

Marketing practices by clinical laboratory sales representatives are governed by several federal laws and regulations. Marketing techniques that would be allowed in other fields are not allowed in the field of lab medicine. Consultant Peter Francis discusses key laws and regulations affecting labs' marketing practices and five things a lab sales and marketing rep should never do. *See p. 2-3.*

Q&A with Gregg Brandush, CMS Division of Clinical Laboratory Improvement and Quality

The Centers for Medicare and Medicaid Services is charged with CLIA oversight and for ensuring that clinical laboratories meet certain quality standards. *LECPR* recently spoke with Gregg Brandsh, RN, JD, Director of the Division of Clinical Laboratory Improvement and Quality, about what's happening with CLIA, CMS survey goals and other lab activities within CMS. *Details on pp. 4-5.*

Data Integrity and Cybersecurity for Labs: How to Minimize Risk of an Attack

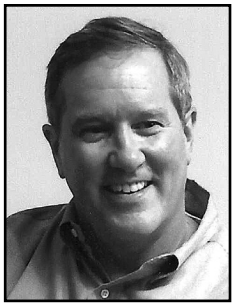
Clinical and anatomic pathology laboratory managers and compliance officers think about risk every day. From what materials to lock up at night, to ensuring availability of reagents and supplies to run tests, every choice made is a balancing act between safety, cost, usability, regulatory compliance and countless other considerations. These tradeoffs apply to the lab's data, too, says Kathryn Rattigan, an attorney with Robinson & Cole LLP (Hartford, Conn.). *Continued on page 6.*

CONTENTS

Key Legal Hotspots for Laboratory Sales and Marketing Reps: Tips on What NOT to Do

By Peter Francis

Following the hiring of a sales representative (whether they come from within the industry or not), one of the first duties of any clinical or anatomical pathology lab is to expose the new employee to the lab's compliance obligations. The lab should provide (1) a copy of the lab's compliance plan and (2) training. Once the materials are reviewed, a written test should be given, either on paper or through a computer program. This compliance training should be presented annually to all lab sales employees and the test results maintained at the lab as documentation.



Peter Francis

The following discussion of compliance in lab sales and marketing equates to a broad overview for general informational purposes. Any legal questions or advice should be addressed to counsel.

Laboratory sales representatives need to abide by a number of laws and regulations, chief among them are the Federal False Claims Act, the Anti-Kickback Statute and the Stark prohibition on self-referrals. There are also considerations related to pricing and supplies. Below we discuss several of these laws and statutes and "don'ts" that sales reps should be aware of. Note that EKRA (the Eliminating Kickbacks in Recovery Act) is outside the scope of this discussion.

The False Claims Act

Watch your step when trying to convince doctors to change their test ordering patterns by suggesting unnecessary tests (singular or within a profile). This gives rise to infringement of the False Claims Act. The 2023 federal penalties are severe: $13,508 to $27,018 per incident. Also, treble damages (three times the amount of actual or compensatory damages) can be enforced either by itself or in addition to civil monetary fines.

The Anti-Kickback Statute

Do not offer money/rebates, gifts, free trips, entertainment tickets, free point-of-care urine test cups, exam gloves or test pricing that is below the lab's cost-of-testing or free testing described as "professional courtesy." Also, do not offer anything of value to someone in exchange for recommending your lab. And do not suggest free pick-up and disposal of biohazard waste from a doctor's office. The penalties for doing any of these things implicate criminal fines up to $100,000, imprisonment up to 10 years and civil monetary penalties up to $100,000. The federal government can also exclude the provider from billing federal programs such as Medicare and Medicaid. This exclusion refers to both the laboratory and the physician caught in the wrongdoing.

Two side notes: (1) the Anti-Kickback Statute ascribes liability to all parties of an impermissible kickback transaction (i.e., the lab, sales rep and the physician) and (2) insurance companies and the federal government frequently combine both the Anti-Kickback Statute and False Claims Act. Prosecutors don't select one over the other if both are implicated. In other words, penalties can get rather expensive.

The Stark Self-Referral Prohibition

The Stark II Law refers to non-monetary compensation. Under this rule (in 2023) a representative may not offer doctors items or services that are valued at more than $489 per year per provider. One might think that if there were four physicians in a group practice, a rep could offer a one-time per year non-monetary compensation gift of $1,956 (e.g., a painting for the waiting room).

This is not the case. Also, any form of non-cash items cannot consider the client's testing volume or be conditioned upon doing business.

In addition—a point rarely understood by lab sales reps—a physician or any member of the doctor's office may not solicit non-monetary compensation (such as lunch) if the representative's lab currently receives Medicare or Medicaid testing referrals from that physician. It is acceptable for the salesperson to initially offer lunch, but not the other way around. Penalties include refund obligation of any overpayment, exclusion from billing Medicare and/or Medicaid and substantial civil money penalties (up to $100,000).

Additionally, there can be fines of up to $100,000 if someone tries to circumvent the law. The Stark Laws fall under strict liability. This means one does not have to prove that someone broke any of the Stark Laws. There are no criminal penalties associated with the Stark Laws.

Due to the direct contact between salespeople and their clients/prospects, lab sales reps are at risk for tripping into the laws that regulate conduct between those who refer and those who receive referrals.

Supplies

Representatives may not offer free items such as biopsy needles, gloves or fax machines to physicians. Nor should they supply free specimen transport items more than the typical specimen volume referred to the lab. If the lab furnishes any type of hardware to a physician that is used for test ordering, specimen preparation or result reporting, the physician should sign and date an equipment loan agreement with the lab.

The contract should state it is prohibited to use the equipment for anything other than the client's testing sent to the lab, and the rep should retrieve the equipment if the physician ceases to be a client. Any paraphernalia should be tagged as property of the lab. Both the lab and the physician should keep a copy of the agreement.

Pricing

If a particular state or insurance plan permits "doctor billing" of lab tests, healthcare providers will probably expect a discount (and/or special pricing on high-volume tests). The Health and Human Services Office of the Inspector General (OIG) may take exception to below fair market prices that are offered in return for federally reimbursed programs.

When a laboratory offers testing at a price that is less than fair market value, the OIG may infer, depending on the facts, that the below fair market value price was offered in exchange for higher paying Federal healthcare program business. Any written proposal that states a discount percentage and/or special pricing should be initially reviewed by the lab compliance officer.

Summary

Due to the direct contact between salespeople and their clients/prospects, lab sales reps are at risk for tripping into the laws that regulate conduct between those who refer and those who receive referrals. Compliance programs exist to reduce the likelihood of inadvertent violation of the fraud and abuse laws.

The penalties for violation of the fraud and abuse laws can be extremely severe. It behooves every laboratory to develop its own compliance plan and ensure that those individuals who interface with clients and prospective customers fully understand the legal rules of the road.

Peter Francis is the president of Clinical Laboratory Sales Training LLC (Woodstock, MD). He can be reached at peter@clinlabsales.com.

Q&A with Gregg Brandush, CMS Division of Clinical Laboratory Improvement and Quality

Congress passed the Clinical Laboratory Improvement Amendments (CLIA) in 1988 establishing quality standards for all laboratories' testing to ensure the accuracy, reliability and timeliness of patient test results, regardless of where the test was performed. The CLIA regulations are based on the complexity of the test method; thus, the more complicated the test, the more stringent the requirements.

Gregg Brandush, RN, JD

The Centers for Medicare and Medicaid Services (CMS) oversees CLIA and is responsible for ensuring that clinical laboratories meet quality standards. *LECPR* recently posed a number of questions to Gregg Brandush, RN, JD, Director of the Division of Clinical Laboratory Improvement and Quality at CMS, about activities within CMS that affect clinical laboratories. Brandush's responses are below.

During the April meeting of the Clinical Laboratory Improvement Advisory Committee (CLIAC), you talked about CMS's CLIA goals for 2023. One of the goals you mentioned was improved processes. Can you elaborate on this?

Access to safe, comprehensive health care is a top priority and responsibility for the Centers for Medicare and Medicaid Services (CMS). CMS is committed to ensuring access to facilities that meet the health and safety quality standards. CMS requires facilities to meet certain health and safety standards to be certified as a Medicare and Medicaid provider.

The CLIA Proficiency Testing—Analytes and Acceptable Performance Final Rule will be implemented on Jan. 1, 2025.

The three major activities of the CMS CLIA Operations are survey, state agency oversight and enforcement. CMS CLIA staff will be collecting data that identifies outliers in terms of survey findings, time spent on survey, team size and other indicators of state performance that will be used to measure effectiveness and efficiency in the implementation of the CLIA program. CMS CLIA staff will be establishing and monitoring adherence to expected timelines, with respect to enforcement action, to ensure that enforcement-related efforts are effective at achieving CMS' goal of quality laboratory testing and patient safety.

In terms of modernizing CLIA, what is happening with the proficiency testing rule implementation?

The CLIA Proficiency Testing - Analytes and Acceptable Performance Final Rule will be implemented on Jan. 1, 2025. [CMS published a final rule related to proficiency testing on July 11, 2022, with an effective date of July 11, 2024. However, in a memo issued May 3, 2023, the agency announced that the new PT requirements would be implemented on Jan. 1, 2025. The rule addresses current analytes and new technologies. It also makes changes to the PT referral regulations to make sure they are aligned with the CLIA statute.]

In March, CMS announced it will begin sending electronic CLIA certificates to labs that opt to receive e-mail notifications. How was this change received? Have most labs opted to receive their CLIA certificates electronically?

CMS CLIA set an initial goal of issuing 10% of CLIA certificates electronically in fiscal year 2023. This would equate to approximately 30,000 electronic certificates. To date, CMS CLIA has

electronically issued more than 17% of CLIA certificates since March 2023. The move towards electronic certificates has largely been received favorably by the laboratory community.

What are CMS' laboratory survey goals for 2023?

The federal monitoring surveys will be focused on assessing consistency in survey findings, efficient use of survey resources and developing plans to address survey related concerns identified in the state survey process. Additionally, CMS annually evaluates and updates survey priorities, as referenced in our survey budget call letter. [Of note, the call letter states that based on national data, a state can anticipate that approximately 3.07% of its labs will receive one or more unsuccessful ratings in FY 2023, with 2.84 proficiency testing failures per laboratory being the norm.]

Can you discuss the certificate of compliance survey findings and what the top deficiencies are nationwide?

The top 10 deficiencies in the nation for CMS surveys can be found on our website for the latest year of data, which is fiscal year 2021. The first chart references the top 10 deficiencies (overall) in the nation for CMS surveys and the second chart references the top 10 conditions in the nation for CMS surveys [The top deficiency is failure to comply with personal competency assessments, and the top condition is failure to comply with proficiency testing requirements]. Specific information related to these deficiencies is found in Appendix C of the State Operations Manual.

Now that the Covid-19 Public Health Emergency has officially ended, are there any requirements for labs to continue reporting Covid test results to any government agencies?

The CLIA requirement that all certificate types report SARS-CoV-2 test results ended on May 11, 2023, when the Public Health Emergency (PHE) was terminated. However, there may be additional reporting requirements that are not enforced by CLIA that could continue to require the reporting of SARS-CoV-2 test results (e.g., state reporting requirements). Laboratories should verify all current guidance before discontinuing the reporting of test results.

Based on national data, a state can anticipate that approximately 3.07% of its labs will receive one or more unsuccessful ratings in FY 2023, with 2.84 proficiency testing failures per laboratory being the norm.

CMS recently issued guidance (memorandum 23-05-CLIA) outlining procedural changes for use of form CMS-116, which is the CLIA application for certification. What are the most recent changes and why were they made?

The information regarding notification in Admin Info: 09-09-CLIA needed to be updated as notification methods have changed significantly since the memorandum was issued in 2008. This memorandum summarizes what laboratory changes require a new Form CMS-116 (CLIA application) to be completed and when written notification of a change is sufficient. We clarified the retention requirements for Form CMS-116. Finally, we included some updated instructions for Certificate Type Changes.

CMS updated the guidance to include email addresses and deleted the guidance for potential fraudulent Form CMS-116 applications. The fraudulent Form CMS-116 information is outdated. Based on lessons learned during the COVID-19 PHE, and in preparation to begin issuing electronic CLIA certificates in 2023, we want to ensure accurate public guidance regarding notification of changes to CLIA certificate information is available to the state agencies, accreditation organizations, exempt states and the laboratory community.

DATA INTEGRITY AND CYBERSECURITY FOR LABS (*cont'd from page 1*)

"Laboratories collect lots of sensitive data," says Rattigan. "Besides employee and payroll information that every business manages, labs rely on the integrity of their test results. Questions about data integrity arising from a security break could throw cold water on relationships with customers, cause reputational harm and lead to costly penalties."

Labs are at risk for cyberattacks, ransomware and other high-profile security attacks, says Rattigan, who suggests that a lab manager or compliance officer start to think about cybersecurity by asking a few basic questions.

- *What do I have?* Not all data is equally valuable or equally high-risk. In addition, some kinds of data, such as medical records and records relating to substance use disorder treatment, trigger different laws with different security, retention and reporting requirements.
- *What happens if I lose it?* Once you've taken stock of what you have, you will better understand the risks you face. Besides regulatory risk, consider factors such as the future value of the data (whether impacting customer relationships or potential sale of the laboratory) or your lab's ability to operate during an IT outage or fulfill its service contracts.
- *How much do I value peace of mind over higher costs?* Experts frame risk in two dimensions, notes Rattigan. Each organization has its own risk tolerance, so consider what measures make sense for your laboratory. "While security safeguards do come at some cost, offsetting the risks to your data and your operations is also important," she explains. "Your approach should satisfy regulators, stockholders and your employees."

Strategies for Reducing Risk

There is no such thing as a zero-risk system, but Rattigan notes that labs can make tradeoffs to mitigate their exposure. For example, a cloud-based data management system may be more feasible if you prefer that a third party manage your data and you want to cut down on upfront costs. But, if data security is a more significant issue than cost, you may consider managing your own data on premises.

Kathryn Rattigan

"The answer really depends on the size of the lab and its needs, budget and staffing," says Rattigan. "There are pros and cons for each."

The pros of using a third party include lower upfront costs, a faster set-up and implementation, separate networks and physical location to help distribute risk and no need to maintain physical hardware. The cons include application program interfaces (APIs) that can be exploited, compliance concerns related to the particular vendor and the vendor's policies and long-term service costs. Third-party APIs present a risk because the business needs to keep certain ports open on its network, increasing its attack surface, explains Rattigan. In addition, a compromised vendor can easily go on to infect the business through the vendor's established link to the business network.

The pros of setting up your own data security system include more in-house control over data management, control over security measures and use of internal network traffic for employee access. Cons include the costs for hardware, software, labor and maintenance; a single point of failure in the event of a denial of service or natural disaster; and the required space for hardware storage.

Other ways of reducing risk without redesigning your entire IT system include purchasing cyber-liability insurance that can be used to cover potential fines and settlements and hiring outside

incident response experts, says Rattigan. The insurance can also potentially cover a ransom in the event of a cyberattack.

"Or, instead of switching to an entirely new system, your organization can explore a hybrid model that keeps the security of physical backups without the overhead cost of managing an entire IT department," she suggests.

Response in the Event of a Data Breach

If your lab does experience a data breach, you should implement your Incident Response Plan. All companies should have a plan and team in place, and you and your staff should have conducted tabletop exercises so you know what to do in the event of an attack, advises Rattigan.

"Anything can be handled better and with more ease if you have practiced enough," she says. "The same idea goes for responding to a data breach or security incident."

Among the first steps you should take:

1. **Secure operations.** This includes physical security, mobilizing the breach response team and speaking with forensic and legal experts.
2. **Fix vulnerabilities.** Review access privileges and check network segmentation.
3. **Notify appropriate parties.** This includes law enforcement, insurers, outside legal counsel and the outside communications team.
4. **Contain the breach.**
5. **Conduct an assessment** to determine what was compromised, who was impacted and what data was affected. Alternatively, engage a third-party forensic firm to conduct the investigation and mitigate the effect of the incident.
6. **Comply with legal obligations** under state and/or federal law (i.e., notification to affected individuals).
7. **Comply with contractual obligations**, such as notifying particular entities.
8. **Conduct a post-incident assessment** so that you can revise processes and procedures to be more effective in the event of future data breaches or security incidents.
9. **Update and implement security safeguards** to protect data and systems moving forward.

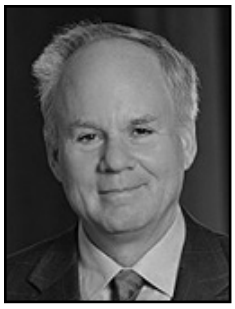
"Think of the lab like the human body: Security is like healthcare—there is no one-size-fits-all approach. It pays to put preventive measures in place and implement an incident response plan before a disaster, not after the threat has already invaded your systems."

Ultimately, making a decision about how to mitigate data security risks is a balancing act between what your lab can afford and how comfortable you are in setting up your own security system, says Rattigan.

"Think of the lab like the human body: Security is like healthcare – there is no one-size-fits-all approach," she suggests. "It pays to put preventive measures in place and implement an incident response plan before a disaster, not after the threat has already invaded your systems."

FDA Preparing to Issue Proposed Rule on LDT Oversight (*con't from p. 1*)

There has been a longstanding discussion regarding oversight of LDTs. Many in the field of laboratory medicine believe that LDTs are already regulated under CLIA, but the FDA has indicated that it believes it has oversight authority over these types of tests. Historically, the FDA has used "enforcement discretion" when it comes to LDTs—employing a hands-off approach to LDTs unless there was a specific need to regulate them.



Jeff Gibbs

However, in recent years the FDA has said that it wants to reconsider its role in oversight of LDTs, noting that it has become increasingly concerned that LDTs may not provide accurate and reliable tests results or perform as well as FDA authorized tests.

In April 2022, for example, the FDA issued a warning about the risks of false positives from noninvasive prenatal tests (NIPTs) that have not been approved by the agency. Jeff Shuren, MD, Director of the FDA's Center for Devices and Radiological Health, said that without proper understanding of how these tests should be used, people may make inappropriate healthcare decisions regarding their pregnancy.

> *"Even if the FDA issues a final rule that survives judicial challenges and is not superseded legislatively, there will be countless issues regarding the interpretation of the rule and its implementation."*

Legislative attempts to place LDTs under FDA oversight failed last year when lawmakers did not pass the VALID Act, which would have explicitly granted FDA the authority to regulate LDTs through a risk-based format. Jeff Gibbs, an attorney with Hyman Phelps & McNamara PC (Washington, D.C.), tells *LECPR* that FDA could incorporate some of the concepts and provisions of VALID in a proposed rule.

"If the FDA is going to expend the resources on a proposed rule, I expect that it would be one with far-reaching consequences for LDTs," he says. "Given Congress' failure to pass VALID last session, FDA's proposed regulation would be in lieu of legislation."

Jon Genzen, MD, PhD, chief medical officer at ARUP Laboratories (Salt Lake City), says he is skeptical that any attempt at rulemaking will definitely clarify the issue of LDTs going forward.

Jon Genzen, MD, PhD

"LDTs are not devices, and applying a device framework to them is not appropriate," says Genzen. "There is still a need for more open debate about how best to address LDTs. I think there is a middle-ground solution that also involves CLIA. It's been eight years since the FDA hosted a public workshop on the issue. I would like to see FDA and CMS [the Centers for Medicare and Medicaid Services] hold joint hearings or workshops."

Gibbs agrees with Genzen that this rulemaking is unlikely to resolve the issue. He notes that the FDA will need to address all substantive comments on the proposed rule, and that if a final rule is issued, it is highly likely that FDA will be sued by opponents of FDA regulating LDTs. In addition, any FDA rule can be overturned legislatively.

"Even if the FDA issues a final rule that survives judicial challenges and is not superseded legislatively, there will be countless issues regarding the interpretation of the rule and its implementation," says Gibbs.

Settlement Highlight Benefits of Self-Disclosure

A recent settlement by a company providing billing services for clinical laboratories highlights the benefits of self-disclosure when noncompliance is discovered.

VitalAxis Inc., a Maryland-based billing company for diagnostic laboratories, has agreed to pay more than $300,480 to resolve False Claims Act allegations that it caused the submission of false claims to Medicare for medically unnecessary respiratory pathogen panels run on seniors who received Covid-19 tests, the Department of Justice (DOJ) announced June 15, 2023.

Labs should be aware that the Department of Justice has been touting the benefits of self-disclosure and has made known that a party who self-discloses may receive a more favorable settlement than a party that does not.

Throughout 2020, VitalAxis performed billing services for a diagnostic laboratory in Atlanta that provided Covid-19 testing to residents of senior living communities. For one chain of communities, the laboratory directed VitalAxis to bill Medicare for respiratory pathogen panels purportedly ordered by a physician who had not actually ordered the tests and who was ineligible to treat Medicare beneficiaries. VitalAxis found the credentials of a different physician and, without authorization, billed Medicare using that physician's name. Medicare subsequently paid the laboratory for these medically unnecessary tests.

VitalAxis received a credit in connection with the settlement in recognition of its cooperation, including by performing and disclosing the results of an internal investigation, disclosing relevant facts and material not known to the government but relevant to the investigation, providing information relevant to potential misconduct by other individuals and entities and admitting liability, according to DOJ.

DOJ Touts Self-Disclosure

Karen Lovitch, Chair of the Health Law Practice and co-Chair of the Health Care Enforcement Defense Practice at Mintz (Washington, DC), tells *LECPR* that VitalAxis might have received a civil investigative demand or subpoena in the context of the government's investigation of the laboratory performing the testing and discovered the noncompliance in the context of responding to it. It is also possible that VitalAxis discovered the noncompliance on its own and made a self-disclosure to the government, she says. That self-disclosure, in turn, could lead to the laboratory being investigated.

Karen Lovitch

"Labs should be aware that the Department of Justice has been touting the benefits of self-disclosure and has made known that a party who self-discloses may receive a more favorable settlement than a party that does not," says Lovitch.

"If a lab is working with a vendor, such as a billing company, that discovers noncompliance involving the lab, the vendor might make a self-disclosure without the laboratory knowing about it. Labs should take steps to be sure that their respective compliance programs are effective, that potential noncompliance is investigated and (if appropriate) reported to the government, and that auditing and monitoring activities are robust and focused on high-risk areas."

OIG Continues to Focus on Medicare Payment to Labs

Several reports published by the Health and Human Services Office of Inspector General (OIG) in the past year focused on Medicare payments to clinical laboratories, a sign that the agency may continue to take a closer look at laboratory testing.

In the OIG's "Semiannual Report to Congress: October 1, 2022—March 31, 2023," the agency noted that it issued 62 audit reports and 19 evaluation reports during the period. The audit identified $200 million in expected recoveries, as well as $277.2 million in questioned costs.

Among the reports that the OIG said were related to Medicare program integrity and financial stewardship:

- Labs With Questionably High Billing for Additional Tests Alongside Covid-19 Tests Warrant Further Scrutiny (OEI-20-00510), December 2022.
- Medicare Part B Spending on Lab Tests Increased in 2021, Driven by Higher Volume of Covid-19 Tests, Genetic Tests and Chemistry Tests (OEI-09-22-00400), December 2022.
- Medicare Could Have Saved up to $216 Million Over 5 Years if Program Safeguards Had Prevented At-Risk Payments for Definitive Drug Testing Services (A-09-21-03006), February 2023.

The OIG also notes that it continues to coordinate with the Department of Justice and criminally prosecute bad actors in the Medicare program. It highlighted two examples of successful criminal prosecutions related to traditional Medicare, one involving an owner and operator of a home health company and one involving a sales representative for a lab.

In the latter case, a sales representative was sentenced to 25 months in prison and ordered to pay, along with yet-to-be-sentenced defendants, a total of almost $3 million for a kickback scheme. The sales rep paid kickbacks to physicians in exchange for referrals and prescriptions directed to select pharmacies and clinical laboratories.

Statistic	***Semi-Annual Reporting Period (10/1/2022-3/31/2023)***
Audit Reports Issued	62
Evaluations Issued	19
Expected Audit Recoveries	$200.1 Million
Questioned Costs	$277.2 Million
New Audit and Evaluation Recommendations	213
Recommendations Implemented by HHS OpsDivs	253
Expected Investigative Recoveries	$892.3 Million
Criminal Actions	345
Civil Actions	324
Exclusions	1,365

Source: HHS OIG

COMPLIANCE 101:

Implementing a Compliance Disclosure Hotline

Clinical Laboratories should keep lines of communication open between employees and the compliance office, advises the Health and Human Services Office of Inspector General (OIG) in its model compliance program for labs. It suggests that labs make available to all employees a hotline telephone number that can be used to anonymously report suspected misconduct.

Laboratories using a hotline should post in common work areas notices describing the hotline and providing the telephone number. Matters reported through the hotline that suggest violations of compliance policies or legal requirements should be investigated immediately to determine their veracity.

CodeMap, a consulting company based in Chicago, suggests the following policy:

> *"Laboratory operates a disclosure hotline, which may be used by all employees, managers and contractors to anonymously report any suspected misconduct or potential compliance issues. Laboratory posts instructions for use of the hotline and the hotline phone number in common work areas. Employees need not worry about retaliation or retribution for using the disclosure hotline.*
>
> *"The Chief Compliance Officer investigates immediately all matters reported through the disclosure hotline. Depending on the outcome of the investigation, Laboratory will institute all necessary corrective actions."*

Benefits of Hotlines

Ethics and compliance hotlines can significantly reduce the chance of whistleblowing in your organization, according to Strategic Management Services (SMS), a healthcare consulting company in Alexandria, VA. If your employees and workforce members do not feel comfortable reporting compliance issues internally, you might consider using an external ethics hotline provider instead.

"Implementing a successful ethics and compliance hotline can create positive effects in the workplace that help improve your compliance program," says SMS in a blog post. "Because your employees know that the hotline is anonymous and secure, you are likely to receive more reports about compliance concerns that may have otherwise gone unreported. This brings potentially serious violations to your attention before they get out of hand."

SMS suggests the following best practices for disclosure hotlines:

- **Multiple reporting channels.** Having both telephonic and web-based reporting systems gives your employees more options for reporting.
- **Around-the-clock-service.** Reporting should be available 24 hours a day, seven days a week for both hotline calls and online report submissions.
- **Confidentiality and anonymity.** All aspects of the system should be confidential and anonymous.
- **Detailed reports.** Whether reports are submitted by a hotline associate or the employee themselves, reporting systems should have answer boxes that prompt detailed responses.
- **Security measures.** Even though a hotline may be confidential and anonymous, the information that is entered in the reporting system still needs to be protected. Security measures should comply with HIPAA security regulations.
- **Multilingual reporting.** Hotlines that offer reporting in both English and Spanish, or other languages, can be more widely used since they accommodate more potential reporters.

CodeMap's Compliance Policy Manual for Clinical Laboratories, 2023 Edition, is available for purchase at www.codemap.com.

In Brief

OIG Recommends CMS Recover Improper Payments for CPT 81408

The Centers for Medicare and Medicaid Services (CMS) did not provide sufficient oversight of Medicare payments for CPT 81408, the genetic-testing procedure code with the second-highest total Part B payments and the molecular pathology procedure with the highest Medicare payment amount ($2,000), concludes a new report from the Health and Human Services Office of Inspector General (OIG). The OIG analyzed Medicare Part B claims associated with payments of $888.2 million for more than 450,000 genetic tests billed under CPT code 81408 that had dates of services from 2018 through 2021. It recommends that CMS direct the appropriate Medicare contractors to review claims billed under this code during the audit period and recover payments that were made improperly.

FDA Requests Input on Increasing Access to Home-Use Health Technologies

The Food and Drug Administration (FDA) is seeking public comment on expanding patient access to medical technologies intended for use by patients in their homes. This effort is part of FDA's 2022-2025 Strategic Priorities focus on advancing health equity. Specifically, the FDA is seeking input on how to support the development of medical technologies, including digital health and diagnostics, for use in non-clinical care settings, such as at home and what processes or technologies would be ideal for transitioning from a healthcare setting to non-clinical care settings.

FDA Launches Cancer Biomarkers Pilot

The FDA on June 20 announced a new voluntary pilot program for certain oncology drug products used with certain corresponding in vitro diagnostic tests to help clinicians select appropriate cancer treatments for patients. Under current policy, the FDA may, in limited circumstances, approve a life-saving treatment that requires use of an in vitro companion diagnostic even if it has not yet received marketing authorization. In these cases, tests offered as LDTS are being used for patient treatment decisions. Through the pilot program, the FDA will request from drug manufacturers performance information for tests used to enroll patients in clinical trials and will post to its website the minimum performance characteristics recommended for similar tests.

Jondavid Klipp, Publisher Kimberly Scott, Editor Jennifer Kaufman, Chief Copy Editor