G2 INTELLIGENCE
A DIVISION OF PLAIN LANGUAGE MEDIA

LAB Compliance Advisor

For Clinical and AP Laboratories and Pathology Practices

June 2021

IN THIS ISSUE

www.G2Intelligence.com

Billing & Coding: OIG Sounds the Alarm on Improper Billing of Lipid Panels & Direct HDL Tests

Medicare could and should have saved over $20 million in payments for medically unnecessary LDL cholesterol blood tests if CMS hadn't been asleep at the wheel for the past five years. That's the gist of the message of a new OIG report that compliance managers need to know about, especially if their labs provide such tests for Medicare patients. Here's a look at the report and what it may portend.

Medicare Coverage of LDL Cholesterol Tests

Medicare Part B covers two basic kinds of cardiovascular-screening blood tests measuring cholesterol and triglyceride levels to detect conditions that may lead to heart attack or stroke:

Continued on page 2

Compliance Perspectives: Beware of Privacy Pitfalls When Remotely Monitoring Lab Telecommuters

Before the pandemic, 80 percent of U.S. employees worked primarily from an external workplace; today, only 21 percent do. Coaxing employees to return to the workplace will be an uphill battle, with recent surveys, including one from Pew Research, suggesting that 54 percent of those who are currently working remotely want to continue spending at least some of their working hours at home. In short, as with other employers, labs need to adjust to the realities of telecommuting. Among the biggest challenges will be maintaining productivity. One potential solution is to deploy technologies that monitor employees' whereabouts and use of computer and other work equipment to verify that employees who work remotely are actually doing their jobs. Unfortunately, doing this exposes your lab to liability risks

Continued on page 9

Billing & Coding: OIG Sounds the Alarm on Improper Billing of Lipid Panels & Direct HDL Tests, *from page 1*

- **Lipid panels** that measure the levels of four lipids in the blood, including total cholesterol, triglycerides, high-density lipoprotein (HDL) cholesterol and low-density lipoprotein (LDL) cholesterol, sometimes called "bad cholesterol"; and
- **Direct LDL tests** that measure the actual level of LDL in the blood.

The level of LDL cholesterol can also be calculated from the results of the other three tests in the lipid panel. As a result, direct testing for LDL cholesterol generally isn't separately reimbursable when the lipid panel is performed for the same beneficiary on the same date of service.

Back in April 1, 2003, CMS added the lipid panel (CPT code 80061) and direct LDL test (CPT code 83721) code pair to its National Correct Coding Initiative (NCCI) edits designed to flag codes that shouldn't be billed together for the same patient at the same time. There are exceptions when it's okay to bill 80061 together with 83721, in which case the lab must add the -59 modifier. However, the expectation is that these cases will be relatively rare.

The OIG Smells an LDL Cholesterol Billing Rat

In a previous audit, the OIG found that the NCCI edit wasn't working and that Medicare was still improperly paying for LDL tests and the lipid panel in circumstances where billing both wasn't justified. It recommended that the CMS tighten up. The purpose of the most recent audit was to determine whether the problem had been solved.

Short answer: No. The OIG audited payments between calendar years 2015 through 2019. Over that four-year period, Medicare Part B made $35.8 million for direct LDL tests to 11,788 providers in addition to lipid panels for the same beneficiary on the same date. After excluding providers with total payments below $500 and interviewing CMS and Medicare Administrative Contractor officials, OIG determined that some providers were billing LDL tests and lipid panels together on a routine basis, i.e., more than 75 percent of the time. Specifically, there were 1,334 such "at-risk providers" accounting for Medicare payments of $20.4 million. After auditing a routine sample, the OIG determined that these payments didn't satisfy the standards allowing for billing lipid panels and LDL tests on the same patient on the same date.

"CMS's oversight was not adequate to prevent improper payments for the direct LDL tests," the OIG concluded. "If CMS had had oversight mechanisms to prevent such payments, Medicare could have saved up to $20.4 million for our audit period."

The OIG Recommendations

The OIG issued two recommendation that CMS order Medicare contractors to:

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.

1. Develop oversight mechanisms to identify and prevent improper payments for lipid panel and direct LDL tests to at-risk providers; and
2. Educate providers on the billing of direct LDL tests in addition to lipid panels.

Perhaps surprisingly, CMS pushed back, indicating that it didn't agree with the first recommendation. Ordering direct LDL tests and lipid panels together is permissible under Medicare payment rules on the basis of the physician's clinical judgment, CMS insisted. The agency was only slightly less happy with recommendation two, noting that it already has issued education on correct coding requirements for the proper use of modifiers on claim lines. We maintain that our finding and recommendations are valid. But OIG held its ground, saying that current education does not address this.

Takeaway

OIG reports like these are frequently followed not just by internal system corrections and education, but also stepped-up enforcement action. However, it appears that CMS isn't going along this time. Foot dragging by CMS might lead OIG to drop the matter, particularly since the dollars involved, i.e., $20.2 million over four years, are so relatively small; on the other hand, the agency may respond by treating the LDL direct tests and lipid panels issue as one that should be primarily pursued at the enforcement level. Stay tuned . . .

Lab Safety: FDA Reverses Course on Lab Worker Re-Use of N95 Masks

For decades, the N95 filtered mask has been a vital piece of personal protective equipment for lab, hospital and other frontline medical workers. But for months, shortages of that precious item which was previously taken for granted left countless health care workers defenseless from exposure to the coronavirus. The good news is that the N95 shortages have finally abated, with surplus stockpiles enough to last three to 12 months. As a result, federal regulators are beginning to unwind some of the health and safety shortcuts they authorized labs to take to deal with the lack of adequate N95 supplies.

The FDA Calls for Ending N95 Recycling & Sharing

National Institute of Occupational Safety and Health (NIOSH) standards dictate that N95 masks be used once and then thrown away. But as an

Continued on page 4

Lab Safety: FDA Reverses Course on Lab Worker Re-Use of N95 Masks, *from page 3*

emergency response to the N95 shortage, the federal government relaxed those restrictions by giving labs and other providers a temporary green light to reuse, recycle and even allow workers to share N95s, provided that proper cleaning, inspection and fit testing measures were performed. Similar temporary compromises were made for other disposable equipment in short supply, including aprons, gowns and swabs.

With some degree of normalcy restored, the government has made moves to go back to the one mask per worker rule. In its mid-April letter, the Food and Drug Administration (FDA) indicated that it's "recommending that healthcare personnel and facilities transition away from crisis capacity conservation strategies."

But labor unions and others concerned about health workers' safety were less than impressed and noted that "recommending" is the operable word. The letter isn't an order and labs are still legally allowed to reuse N95s.

But federal officials suggest that this may change soon. Suzanne Schwartz, director of the FDA's office of strategic partnership and technology innovation says that "the ability to decontaminate was purely a last resort, an extreme measure." Schwartz said we "need to move back towards contingency and conventional strategies, which is, you use the respirator for the interaction, and then you dispose of it and get a new one." She also suggested that NIOSH and the Occupational Safety and Health Administration (OSHA) feel the same way on this.

Takeaway

The N95 reuse and recycle rules are clearly on borrowed time. Still, it's a headscratcher why the peel back of such a dangerous policy adopted as an expediency in response to a crisis that apparently no longer exists, namely, the N95 mask shortage, is taking so long.

CDC Tweaks N95 Mask Guidance

The U.S. Centers for Disease Control (CDC) made a subtle but significant adjustment to its N95 medical mask guidelines that you might not have noticed. Previously, when N95s were in desperately short supply, the CDC said that they should "be reserved" for healthcare workers. But on April 9, the CDC modified its position by indicating that N95 masks should be "prioritized" for healthcare workers but also giving the nod to bulk sales for use at other high-risk workplaces, such as schools, travel and retail.

Quiz: Who Has OSHA Responsibility for the Health & Safety of a Temp?

What are your OSHA duties to temporary workers ("temps") whom you hire from a temp agency to work at your lab? Stated differently, are you or the temp agency responsible for the temp's health and safety? Here's a set of scenario quizzes that illustrate how the rules work.

SCENARIO 1: RESPONSIBILITY FOR HAZCOM TRAINING

The Temps R'Us Agency (Agency) assigns an employee to temporary work at XYZ Laboratories (Labs). Agency is perfectly aware that knows that Labs' workers handle and use hazardous chemicals for testing operations. But the temp has no Hazcom training whatsoever. As a result, he suffers an injury as a result of exposure to a toxic chemical while working for Labs.

QUESTION

Who's responsible for providing the temp the required Hazcom training?

A. Agency
B. Labs
C. Both
D. Neither

ANSWER

C. Both the Agency and Labs face potential fines for failing to provide the temp Hazcom training.

EXPLANATION

In a 1994 Interpretation Letter, OSHA made it clear that where a temporary employment agency sends one of its employees to a client site that the agency knows or should know exposes the employee to chemical dangers (which is clearly the case in this scenario), it considers both the agency and client responsible for ensuring that the temp has the required Hazcom safety training and information. According to OSHA:

- The temps agency would be expected to provide the temp general training about Hazcom, labels, SDSs, etc. required; and
- The client would be responsible for providing the temp site-specific training, e.g., where the SDS binder is kept, what hazardous chemicals the temp will be exposed to, what PPE is required to prevent illness or injury, etc.

OSHA confirmed that this remains its position in a 2012 Interpretation Letter.

SCENARIO 2: PPE

Same situation as above. But now assume that the temp is working in an

Continued on page 8

Quiz: Who Has OSHA Responsibility for the Health & Safety of a Temp?, *from page 5*

operation that requires eye and face protection but isn't furnished the right equipment, let alone instructed how to use it. As a result, she suffers an avoidable injury when a caustic chemical splashes into her eye.

QUESTION

Who's responsible for providing the temp the required eye and face protection?

A. Agency
B. Labs
C. Both
D. Neither

ANSWER

B. Labs is responsible.

EXPLANATION

According to that same 1994 Interpretation Letter, client employers are responsible for providing PPE for site-specific hazards to temps. However, the Letter leaves open the possibility of holding the temp agency accountable for not including in its contract with the client employer an express provision requiring the client to provide the temp whatever PPE is required to do the job.

SCENARIO 3: MEDICAL SURVEILLANCE

Let's now assume that the temp will be involved in work operations involving hazardous concentrations of a hazardous product for which medical monitoring is required.

QUESTION

Who's responsible for performed the required medical evaluations and monitoring of the temp?

A. Agency
B. Labs
C. Both
D. Neither

ANSWER

C. Both Agency and Labs have responsibilities for medical monitoring of the temp.

EXPLANATION

Here's how OSHA divvies up the responsibilities:

- The client employer must offer and perform the required medical surveillance or evaluations and keep the required medical records;

- The temp agency is responsible for making sure that the client employer meets these responsibilities and that all of the required tests and monitoring are carried out and properly documented;
- The agency is also required to maintain cumulative exposure and medical monitoring records where the temp is exposed to hazardous substances requiring monitoring at more than one client employer site.

TOOL

MODEL LAB EMPLOYEE REMOTE MONITORING OF TELECOMMUTERS POLICY

Letting employees telecommute poses significant operational and management challenges to labs, not the least of which is ensuring that employees are actually doing their jobs and meeting expected productivity standards when working from home. Software, apps and other monitoring technology can go a long way in meeting this goal; but it can also get you into hot water under privacy and other laws. The best way to manage privacy liability risk is to include specific language in your telecommuting policies and arrangements that provides for monitoring. The idea is to let employees know exactly what you're going to do and how, and ensure they don't have reasonable expectations in the information collected. Here's some model language you can adapt for your own use.

IMPORTANT NOTICE TO LAB EMPLOYEES SEEKING PERMISSION TO TELECOMMUTE OR WORK REMOTELY OFF SITE

1. POLICY

In consideration for being allowed to work from home or another remote location, employees acknowledge and agree that XYZ Laboratories may use software applications and other forms of monitoring technology ("monitoring technology") in accordance with the rules set forth in this Policy.

2. PURPOSES

XYZ Laboratories will use monitoring technology for the sole purpose of:

- Ensuring telecommuters' health and safety in accordance with XYZ Laboratories' obligations under the Occupational Safety and Health Act and regulations and other applicable laws;
- Verifying that telecommuters are meeting XYZ Laboratories' expectations for employee availability, attendance, productivity, engagement and dress code, as set forth in the Telecommuter Agreement;
- Documenting work hours, overtime, breaks and other records XYZ Laboratories is required to maintain under [state] employment standards laws; and
- Ensuring the confidentiality of its proprietary business information and trade secrets.

3. COLLECTION, USE & DISCLOSURE OF INFORMATION

3.1 Monitoring Technology

XYZ Laboratories will use the following monitoring technology to collect the information provided for in this Policy: [List technology and how it works]

3.2 Information Collected

XYZ Laboratories will use the monitoring technology to collect the following information: [List each kind of information to be collected]

3.3 Use of Information Collected

XYZ Laboratories will collect only the minimum amount and type of information it reasonably needs to accomplish the purposes set forth in Section 2 above. [list specific applications]

Continued on page 8

MODEL TOOL: Lab Employee Remote Monitoring of Telecommuters Policy, *from page 7*

4. CONFIDENTIALITY

XYZ Laboratories will keep the information it uses monitoring technology to collect and disclose it only to the telecommuter's supervisor, manager and other authorized to access and use the information for purposes of carrying out their respective roles and responsibilities under the Telecommuter Agreement and where disclosure is required under applicable laws and standards.

5. DESIGNATED CONTACT

Employees who have questions or concerns about this Policy, the information it covers and the collection, use and disclosure of that information may contact [list contact person].

6. ACCOMMODATIONS

Failure to sign the acknowledgement below will be grounds to revoke the employee's permission to telecommute. Employees seeking accommodations to this Policy may submit an accommodations request by [describe procedures].

• • •

EMPLOYEE ACKNOWLEDGEMENT AND CONSENT

I hereby acknowledge that I have read and understood and consent to the collection, use and disclosure of my personal information by XYZ Laboratories to monitor my health, safety and job performance as a condition for being permitted to work from home as provided for in the XYZ Laboratories Telecommuter Agreement.

Employee Name: _____

Date: _____

Signature: _____

Compliance Perspectives: Beware of Privacy Pitfalls When Remotely Monitoring Lab Telecommuters, *from page 1*

under privacy and other laws. Here's a look at the risks and how to manage them.

Remote Monitoring & Teleworker Productivity

Remote monitoring technology may include apps that employees upload onto their personal computers and network software that can monitor the network, internet, and email usage of a large group of employees to collect data showing when they're idle, how often they surf the internet, how and how often they email and make phone calls, etc.

In addition to helping maintain telework productivity, these solutions enable labs and other organizations to protect confidential business information and keep work hour, overtime and other records required by federal and state labor standards laws.

Remote Monitoring & Telecommuter Privacy

Labs need to be aware that use of remote monitoring solutions may run afoul of employees' privacy rights under the following laws.

Federal ECPA Law

The main federal law that comes into play when labs remotely monitor employees who work from home is the *Electronic Communications Privacy Act of 1986* (ECPA), including:

- Title I of the ECPA, aka the Wiretap Act, which makes it illegal to intentionally intercept, use, disclose or otherwise obtain any wire, oral or electronic communication;
- Title II, the Stored Communications Act, which requires maintaining the privacy of stored electronic information; and
- Title III, which regulates pen registers and trap or trace devices that record identifying information about communications, e.g., the phone number dialed, but not their actual substance.

While these ECPA restrictions would seemingly ban employer monitoring of telecommuters, they're also laden with exceptions. The most important of these is the business use exception, which allows employers to monitor employees' oral and electronic communication, as long as they do so for a legitimate business reason. In addition, the ECPA doesn't protect the privacy of stored information on the employer's own servers or equipment. Last but not least, it also leaves the door open for employees to consent to the employer's collection, use and disclosure of their protected information.

Continued on page 10

Compliance Perspectives: Beware of Privacy Pitfalls When Remotely Monitoring Lab Telecommuters, *from page 9*

State Privacy Laws

Some states have their own, more restrictive personal privacy laws that may apply to remote monitoring of lab employees. For example, some states like California, Maryland and Illinois, have "two-party consent" laws requiring everyone involved in a phone call or electronic communication to consent to its monitoring. Other states, including Connecticut and Delaware, require employers to give employees notice that they're being monitored before monitoring can take place.

Contract & Labor Law

Telecommuters may also have reasonable expectations of privacy under their collective bargaining agreement (CBA) or individual employment contract. In addition to violating the CBA, the National Labor Relations Board has issued case rulings finding that use of cameras and surveillance technology on employees constitutes an unfair labor practice, at least to the extent it occurs while they're engaging in organizing or union-related activity.

Common Law

Another potential source of employee privacy rights is "common law," or non-statutory law made by judges in deciding court cases. Cases have found that use of surveillance technology to spy on employees may constitute a tort such as intentional infliction of mental distress. Routine use of remote monitoring solutions to manage telecommuters probably wouldn't cross the line. To rise to the level of intentional infliction of mental distress, the privacy violation would have to be pretty flagrant. Specifically, the telecommuter being monitored would have to prove that:

- The employer engaged in not just privacy-invasive but "outrageous" conduct;
- A reasonable person would consider the invasion highly offensive and causing distress, humiliation or anguish; and
- The employee actually did experience distress, humiliation or anguish.

4 Ways to Keep Remote Monitoring Solutions Compliant

If your lab uses or is thinking about using technology to monitor employees who work remotely, you need to ensure that you do so in a way that doesn't get you into legal trouble. The problem is that this is a new area of the law and we don't have any cases or official guidelines specifically addressing how to do that. The best source of guidance we have is indirect in the form of analogy to the rules that courts and arbitrators ("courts") have used to evaluate the legality of cameras and other workplace surveillance technology.

1. Use Must Be Reasonable

Rule of Thumb: Employers can collect, use and disclose personal information only for purposes that a reasonable person would consider appropriate under the circumstances. Courts typically use a four-part test to determine whether use of surveillance technology is reasonable and appropriate:

- The use of the technology must be demonstrably necessary to meet a specific need;
- The technology must be likely to be effective in meeting that need;
- The loss of privacy to the employees being monitored must be proportional to the benefit gained; and
- There must be no less privacy-invasive way of achieving the same end.

We know from surveillance technology cases, that courts are more open to use of privacy-invasive technology in the workplace when it's used for health, safety and security purposes.

Example: A court found that a locomotive company's use of surveillance cameras to safeguard employees' health and safety after a number of safety incidents was reasonable.

Example: A court found it reasonable for an employer to install a GPS in employees' vehicles to promote safe driving and ensure compliance with OSHA laws.

Remote monitoring solutions can be used to ensure a telecommuter's health and safety while working from the lab, of course; but their primary purpose is to monitor telecommuter performance or productivity. Historically, courts have been reluctant to allow employers to install cameras, GPS and other privacy-invasive surveillance solutions for such purposes.

Example: A food company installed surveillance cameras in its factory to monitor who entered and exited the plant, trace sources of food contamination and prevent theft. The union contended that use of the surveillance cameras was unreasonable and violated employees' privacy rights under the collective agreement. After balancing the employer's interest in security and food safety against the employees' privacy expectations, the court ordered the employer to remove the cameras in the food production areas while allowing it to keep the cameras at the entry and shipping areas in place.

Example: A court concluded that an internet service provider's use of surveillance cameras to manage the productivity of its sales, marketing and technical support staff was unreasonable because there were less privacy-invasive alternatives available.

Continued on page 12

Compliance Perspectives: Beware of Privacy Pitfalls When Remotely Monitoring Lab Telecommuters, *From Page 11*

It remains to be seen whether the prevalence of telecommuting will cause courts to loosen up and give labs and other employers more leeway to perform monitoring for productivity purposes.

2. Information Collected Must Be Kept to Minimum

Another key factor is what and how much personal information the employer collects to monitor telecommuters remotely. Collection must be limited only to the information necessary to accomplish the purpose of deploying the technology and not include non-work-related personal information in which telecommuters have reasonable expectations of privacy. Accordingly, software or apps that tap into lab employees' personal calls, emails or computer use will be highly problematic.

Courts will also consider the kind of technology used. Spyware and technologies that enable labs to intercept communications, scan or capture images for content, monitor keystrokes or covertly listen into phone calls are particularly invasive and likely to raise privacy red flags.

3. Telecommuters May Need to Consent

Employers generally need consent to collect, use or disclose employees' personal information. But there are exceptions. As noted above, the exceptions under the federal ECPA are pretty broad and require nothing more than a legitimate business purpose. However, consent requirements may be much stricter under state laws. As has proven the situation with use of surveillance cameras, the two exceptions most likely to justify use of remote monitoring technology without employee consent include:

- Getting consent would compromise the availability or accuracy of the information collected; and
- The collection of the information is for the purpose of investigating violations of the employment agreement or the law.

Of course, exceptions are unnecessary when employees give their consent freely. This might be the situation with remote work to the extent that employers are in the position to require employees to consent to being tracked in exchange for permission to telecommute. Such consent would probably be legally valid, provided that it clearly spells out what information will be collected and how it will be collected and used.

4. Telecommuters Must Know They're Being Monitored

Remote monitoring technology is more privacy-invasive when you use it surreptitiously without employees' knowledge. For example, in a 2005 case, a court ruled against an employer that secretly installed keystroke logging software on an employee's work computer to monitor productivity. Information allowing an employer to know how employees use their work

time may be necessary for employee management, the court reasoned. However, the keystroke software overreached and collected unnecessary information for employee management purposes.

Solution: Create a Written Telecommuter Monitoring Policy

The best way to manage privacy liability risk is to include specific language in your telecommuting policies and arrangements that provides for monitoring. The idea is to let employees know exactly what you're going to do and how and ensure they don't have reasonable expectations in the information collected. Like the template on page 8, your policy language should, at a minimum:

- Explain the purposes for which you use remote monitoring solutions;
- Describe the actual solutions you use and how they work;
- List the specific kinds of information to be collected, which should correspond to the attendance, performance and productivity standards that you'll use the data to monitor;
- Indicate who will have access to the information and how they'll use it;
- Require lab employees to accept and consent to these terms in exchange for being allowed to telecommute;
- List a contact person or office where employees can direct their questions or concerns; and
- Provide for accommodations to the policy in accordance with federal and state anti-discrimination laws.