G2 Compliance Advisor

For Clinical and AP Laboratories and Pathology Practices

G2 INTELLIGENCE
A Bloomberg BNA Business
Bloomberg BNA

September 2014

Inside this issue

www.G2Intelligence.com

Wall Street Journal Article Illustrates Increased Compliance Risks for Labs

Health care fraud, waste, and abuse, and their impact on health care costs and patient care, is a very public issue in 2014 as several clinical laboratories found out the hard way when the *Wall Street Journal* (*WSJ*) recently named them in an article about the federal anti-kickback laws.

This article's intent is to highlight the compliance risks that laboratories now face as the government improves its ability to detect fraud and abuse in health care, primarily as a result of data mining expertise and the public release of health care claims and quality information.

Brief Background

The *WSJ* article focused on one laboratory in Virginia, Health Diagnostic Laboratory Inc. (HDL), but named several others, that paid physicians who sent blood samples to their laboratory for testing. The fees were said to cover the cost of collecting the blood sample or, as in the case of HDL, to cover the costs of processing and handling those samples.

Some of the labs, including HDL, said they believed it was a long-standing, industrywide practice, but that is not necessarily the case. Most labs, including the nation's largest labs, do not routinely pay such fees. Other labs named in the story were Quest's Berkeley HeartLab,

Continued on page 2

Medicare Provides Details on How to Bill For Hepatitis C Screening

The Clinical laboratories should pay close attention to two new Medicare transmittals that explain how to bill for the new hepatitis C virus (HCV) screening benefit since claims that violate frequency or diagnosis code requirements will result in payment denials.

The Centers for Medicare and Medicaid Services (CMS) transmittals, released Sept. 5, explain how to bill for the HCV screening benefit and incorporate the new national coverage determination in the Internet Only Manual Publication 100-03, *Medicare National Coverage Determinations*. Transmittal R3036CP explains the billing requirements and updates the *Medicare Claims Processing Manual* (Publication 100-04). Transmittal R174NCD updates the *Medicare National Coverage Determination Manual* (Publication 100-03).

Continued on page 9

Wall Street Journal Article Illustrates Increased Compliance Risks for Labs, *from page 1*

Singulex Inc., Boston Heart Diagnostics Corp., and Atherotech Diagnostics Lab. It should be noted that according to the story, Berkeley HeartLab stopped paying the fees after it was purchased by Quest Diagnostics.

The Government View

The government sees the fees as suspect and meant to provide a financial incentive to refer tests to the lab paying the fees. The *WSJ* article says the labs are under investigation by the Department of Health and Human Services Office of Inspector General (OIG) and the Justice Department but did not elaborate on the investigation, saying only that the agencies declined to comment. As part of that investigation, the OIG issued a special advisory opinion on June 25 that provided guidance to the industry indicating such payments "present a substantial risk of fraud and abuse under the anti-kickback statute."

According to the CEO of HDL, Tonya Mallory, the fraud alert is new guidance and HDL stopped the payments shortly after it was issued. The other labs also stopped the payments. While Mallory repeatedly says that HDL has done nothing wrong and says it will vigorously defend itself if formal charges are made, the damage may already have been done through the reputational harm generated by the article.

In a Sept. 23 updated *WSJ* article, Mallory reportedly resigned. HDL will be led by its co-founder, Joe McConnell, formerly a Mayo Clinic scientist, going forward. Mallory will remain on the board of directors and serve as an adviser to McConnell.

Some Data Released Available Through CMS

The article cites specific data that it implies raises questions about HDL's practices and motives. Some of the data and statistics used in the story are taken directly from data CMS made public last April. A hyperlink embedded in the article takes the reader to a series of spreadsheets specific to HDL showing billing and reimbursements for most, if not all, of its tests. Here are a few examples:

The article cites specific data that it implies raises questions about HDL's practices and motives. Some of the data and statistics used in the story are taken directly from data CMS made public last April.

- HDL received 64 percent of all Medicare payments for its top nine tests;
- For one procedure, a method code for an electrophoretic procedure, HDL received 93 percent of all the money Medicare paid for that procedure in all of 2012 for all labs;
- The electrophoresis procedure earned HDL $11.9 million in 2012 while the total for all other labs combined was $850,000; and
- HDL received $139 million in Medicare payments in 2012.

Another issue for HDL described in the article concerns the performance of a new test designed to measure a patient's sensitivity to the blood thinner Plavix. The test was performed on samples previously stored by HDL. After concerns were raised by employees of HDL saying it was inappropriate to perform so many of them when the test has limited application, the article alleges that Mallory instructed that the tests be performed anyway as long as there was a physician order for it.

How Is the Article Viewed by a Laboratory Compliance Professional?

If HDL is truly under investigation by the government, there are a variety of issues it may face beyond the anti-kickback issues for the processing and handling fees it pays its referral sources.

First, let's consider those fees in light of the Stark regulations. Stark would consider the fees remuneration. If a lab is paying remuneration to a physician who refers to it, the payments must fit within a Stark exception and meet all the criteria for that exception, not the least of which is fair market value (FMV) for the services. HDL

says it is paying FMV, but when compared to the fees other labs named in the article are paying, it is paying more than any of them. In an investigation, HDL would be required to show exactly how it determined the FMV for the service.

In the article, there is no mention of written agreements between HDL and each of the referral sources, which is the first criteria for both the anti-kickback statute safe harbor and the Stark exception covering payments. We don't know whether HDL had those agreements in place, but if there are no written agreements, both laws have been violated.

Another practice that raises flags for a compliance professional is that HDL promotes the use of custom panels and profiles, a practice that most labs have shied away from since the publication of the OIG's compliance guidance for labs in the *Federal Register* in August 1998. HDL makes no mention of physician acknowledgements for the custom panels. Physician acknowledgements are considered essential if a lab offers any custom panels to its clients.

Labs need to fight fire with fire. They should do their own comparative data audit using the 2012 Medicare provider utilization and payment data provided by Medicare at www.cms.gov (look under "Research, Statistics, Data & Systems").

What Can Labs Do to Defend Themselves

Understand that under the current enforcement climate, anything your lab does has greater potential to be discovered than at any time in its history. For several years, laboratory consultants and billing and compliance experts have been pointing to data mining as one of the more important issues facing laboratories and other providers in the future, and the future may well be here. The HDL story, still unfolding, is a perfect example of the consequences of transparency in provider pricing and billing, and the effects of data mining and analysis. It has all of the key elements of such a case, including a media story in a national newspaper and a government investigation likely based in part on data mining and analysis techniques.

Labs need to fight fire with fire. They should do their own comparative data audit using the 2012 Medicare provider utilization and payment data provided by Medicare at *www.cms.gov* (look under "Research, Statistics, Data & Systems"). The first step is to find the information on your own lab. You will have to know the name used to identify your lab to find your data. Once the data is located, prepare a spreadsheet of just your data. The spreadsheets you will be comparing to are the sheets where data is aggregated for all providers. Look for anything that makes your lab standout from the aggregate data.

Labs should also include some kind of data mining or data review of their claims as a routine component of their auditing and monitoring plan.

Takeaway: Government auditors and investigators are becoming increasingly more sophisticated in their use of claims data to identify problem providers and suppliers. It is up to the provider community to develop their own data analysis techniques to keep up and detect potential problems before the government does. G2

When It Comes to HIPAA Security, Trust No One

A Huntsville, Ala., laboratory learned the hard way that it must take whatever steps necessary to ensure its business associates are complying with the Health Insurance Portability and Accountability Act (HIPAA) requirements, including conducting periodic audits.

Diatherix Labs reported a HIPAA breach of more than 7,000 patient records after it discovered a contractor, Diamond Computing Co., allowed access to one of its servers through Google. The server contained patient billing documents, health insurance forms, patient names, and addressees. Many of the documents also included patient Social Security numbers, dates of birth, diagnoses codes, and diagnostics tests

ordered. There was, however, no exposure of credit card or banking information and test results. The information was exposed for nearly three years starting Sept. 24, 2011, until Diamond terminated access to the server on July 10 at Diatherix's request.

Diatherix Bears the Cost and Bad Press

In a notice posted on its Web site, Diatherix says that it conducted an investigation after discovering the breach, but it does not go into any detail of how it actually learned of the exposed server. It does note that it hired an outside data security firm to aid in the investigation. The lab commented that its investigation revealed that the server was first accessed on Oct. 16, 2011, but no protected health information (PHI) was viewed.

The first time documents containing PHI were viewed was on March 7, 2014, says the lab. Diatherix notified 7,016 patients on Aug. 7 that the breach had occurred and offered to pay for a one-year protection plan to help prevent identity theft through Experian, a national credit reporting agency. It also set up toll-free lines where it says concerned patients can find out if their information was affected and to get more information about the Experian plan.

Diatherix had to notify the U.S. Department of Health and Human Services about the breach. It also notified the appropriate state agencies. The lab's name was on the letters and public notices about the security lapse, not Diamond's. Every story in the public media researched for this article lead with Diatherix's name.

The lab's name was on the letters and public notices about the security lapse, not Diamond's. Every story in the public media researched for this article lead with Diatherix's name.

Diatherix also had to contact Google and other search engines that may have had access to the server and ask them to remove any PHI they might have.

Other steps Diatherix took besides those already mentioned included confirming that Diamond had destroyed or secured all of the PHI from its patients stored on the exposed server. Finally, it initiated a security review of other similar vendors to confirm their security procedures. Diatherix says in its notice, "Our organization takes information security and patient privacy very seriously. We deeply regret this situation and any inconvenience this may cause our patients."

Steps to Take to Reduce Your Risk

If your laboratory hasn't already done so, it should compile a list of any vendors who have access to your patient's PHI with the intention of conducting audits and confirming their security measures. Don't take their word for it, ask for a copy of their written plan and the results of audits or security assessments they have conducted.

If your internal security officer does not have the expertise to review their plan and develop and conduct audits of those vendors, make sure he or she gets the training needed or plan on hiring an outside security firm to help.

Make sure there are provisions in your contracts and agreements that allow you the right to audit vendors and other associates. Also, try to include language that would hold them financially accountable for a security breach that they actually cause or allow to happen.

Plan ahead by making sure your privacy and security officers have a plan to address breaches, including the steps necessary to conduct an appropriate and thorough investigation. Budget funding for potential breaches and their associated costs.

Takeaway: In the case of a security breach, the entity that owns the PHI is going to bear the cost and reputational harm associated with it. It would be prudent to plan ahead for such an incident, including budgeting for it and ensuring your security officer is well trained.

G2 INTELLIGENCE
A Bloomberg BNA Business
Bloomberg BNA

COMPLIANCE PERSPECTIVES

Robert E. Mazer, Esq., is an attorney with Ober|Kaler in Baltimore.

Medicare Medical Necessity Requirements Continue to Vex Clinical Laboratories

For more than a quarter century, clinical laboratories have struggled with the Medicare program over application of medical necessity requirements to laboratory services. The issue is complicated because, most frequently, a laboratory claims payment for the services, but the tests were ordered by an unrelated physician. This results in tension among various Medicare statutory principles: The Medicare program pays only for services that are reasonable and necessary to diagnose or treat an illness or injury,[1] and Medicare providers are required to furnish documentation to support Medicare payments due them.[2] However, under limitation of liability and related "without fault" provisions discussed below, a provider is to be protected from financial liability when it did not know or have reason to know that payment for its services would be denied based on lack of medical necessity.

The specific nature of medical necessity disputes has changed since the early years of Medicare because clinical laboratories are now required to submit a diagnosis code on Medicare claims for payment, and ordering physicians are required to provide laboratories with diagnosis or other medical information required for the laboratory to receive payment.[3] Additionally, national coverage determinations (NCDs) and local coverage determinations (LCDs) frequently provide laboratories with some ability to determine, in advance, whether Medicare will consider a test to be medically necessary.

We will address below Medicare medical necessity requirements, Medicare financial liability protection provisions and related principles, and the application of these principles by courts and the Department of Health and Human Services (HHS), of which the Centers for Medicare and Medicaid Services (CMS) is a part. We then offer suggestions as to how a clinical laboratory may reduce loss of revenues from tests later determined to lack medical necessity.

Medicare Medical Necessity Requirements

It is well-recognized that a test can be found not "reasonable and necessary" if it is determined to be not medically necessary given the patient's diagnosis or condition.[4] In addition, a claim for a clinical laboratory test can be denied as not reasonable and necessary if the test is determined to be not safe and effective or if it is considered experimental or investigational.[5] There are, however, numerous other bases on which a laboratory test can be found to be not reasonable and necessary. This might be the

1. 42 U.S.C. § 1395y(a)(1)(A).
2. 42 U.S.C. § 1395l(e).
3. 42 U.S.C. § 1395u(p)(4). Although this statutory provision does not expressly provide for penalties, at least one Zone Program Integrity Contractor has indicated that a referring physician's failure to provide the required documentation may result in revocation of its Medicare enrollment and billing privileges.
4. *See* Medicare Program: Negotiated Rulemaking: Coverage and Administrative Policies for Clinical Diagnostic Laboratory Services; Final Rule, 66 Fed. Reg. 58788, 58792 (Nov. 23, 2001).
5. Medicare Program Integrity Manual ("MPIM"), §§ 3.6.2.2, 13.5.1.

case if the test was not "ordered" in accordance with Medicare requirements, if the physician ordering the test was not the "treating" physician, or if the ordering physician did not use the test results to diagnose or treat the patient's specific medical problem.[6]

In many cases, the completed test requisition—the only information available to the laboratory prior to performance of the test—will not provide any indication that the requested test was not reasonable and necessary. In fact, based on the diagnosis information provided by the physician, it may appear that the test requested satisfies medical necessity requirements as specified in an NCD or LCD. However, the medical records maintained by the ordering physician may fail to support coverage of the test. As part of a post-payment audit, it may be determined that the test "order" was not reflected in the patient's medical record, the medical record entry was not properly authenticated, or the content of the medical record did not support the diagnosis code included on the requisition. At least one Medicare contractor has found medical records inadequate when they did not explain the reason that certain tests were ordered, i.e., provide a "nexus" between the patient's signs and symptoms and the tests that were ordered.

Medicare Financial Protection Provisions

The Medicare statute includes limitation of liability provisions which indicate that when services furnished by a provider are determined not to be reasonable and necessary, Medicare will nevertheless pay the provider for its services, so long as neither the individual for whom the services were furnished nor the provider knew, or could reasonably have been expected to know, that Medicare would not reimburse the items or services in question.[7] The Medicare statute also provides that overpayments should not be recovered from a provider if it was "without fault," i.e., if it exercised reasonable care in billing and accepting Medicare payment.[8] This requires that the provider have made full disclosure of all material facts and that, based on the information available to the provider, it had a reasonable basis for assuming that the payment that it received was correct. Medicare administrative contractors and other Medicare auditing organizations are specifically required to make a limitation of liability and "without fault" determination when a claim is denied because an item or service is not reasonable and necessary.[9]

As part of a post-payment audit, it may be determined that the test "order" was not reflected in the patient's medical record, the medical record entry was not properly authenticated, or the content of the medical record did not support the diagnosis code included on the requisition.

Application of Statutory Principles

Based on the limitation of liability and "without fault" authorities discussed above, clinical laboratories would appear to have a strong argument that they should not be required to forego payment for services that are determined not to be reasonable and necessary—or to repay amounts previously received from Medicare—when the only basis for denial of the claims is the content of the physician's medical records. In earlier years, these arguments appear to have been accepted frequently. These arguments have not fared nearly as well in recent years, although the controversies have frequently related to items or services other than clinical laboratory tests.

This appears to be true for at least three reasons. First, in several cases, there may have been significant question whether the provider furnishing the services was

6. *See* 42 C.F.R. 410.32(a).
7. *See* 42 U.S.C. § 1395pp(a).
8. 42 U.S.C. § 1395gg(b); *see also*, Medicare Financial Management Manual, Ch. 3, § 90.
9. MPIM, § 3.6.2.3.

independent of the ordering physician, such that it actually had no reason to believe that the services ordered by the physician were not medically necessary. Second, the Medicare Appeals Council and courts reviewing its decisions have permitted the statutory obligation of the entity seeking Medicare payments to provide documentation supporting its claims to trump any argument based on the supplier's lack of knowledge of the reasons for which the test was ordered, how the results were used, or its lack of access to related medical record documentation. Additionally, even though regulations require only that the laboratory maintain documentation received from the ordering physician and documentation demonstrating that its Medicare claim accurately reflected that information, a laboratory's failure to provide additional documentation supporting medical necessity has resulted in denial of claims for payment.[10]

CMS Understands the Laboratory's Problem

In one recent decision involving tests furnished by an independent diagnostic testing facility (IDTF), the council stated that the "entity submitting the claim for its services will not receive Medicare coverage . . . unless the services are documented as reasonable, necessary, and otherwise in compliance with Medicare requirements." The council recognized that "providers of laboratory . . . services are dependent upon the ordering physicians to provide part of the documentation required to obtain Medicare coverage for their services." Nevertheless, it held that the IDTF was financially responsible for the services that it furnished when it was unable to provide documentation to support their medical necessity. According to the council, "Medicare's documentation requirements are not intended to make . . . laboratories . . . the reviewers of the medical necessity, but rather require those entities, if they are going to bill Medicare, to support their claim for payment with documentation showing that the service is a service covered by Medicare."[11]

In an appellate decision frequently cited by HHS, the court relied on regulations stating that a provider is deemed to know the content of manual issuances, bulletins, and other written guidelines provided by CMS or the Medicare contractor.

Second, findings that a provider knew or had reason to know that a claim would be denied have been supported by the thinnest of reeds. In an appellate decision frequently cited by HHS, the court relied on regulations stating that a provider is deemed to know the content of manual issuances, bulletins, and other written guidelines provided by CMS or the Medicare contractor. According to the court, since these guidelines indicated that the supplier was responsible for supporting medical necessity with documents that were generally in the possession of the ordering physician, it had sufficient notice that Medicare might require such documentation and would deny the claim if it was not provided.[12] Therefore, although the court did not find explicitly that the provider knew or could have been expected to know "that payment would not be made," it upheld the council decision that the supplier would not receive protection under limitation of liability provisions.

The council has also found that an IDTF had reason to know that its claim would not be paid because the contractor's denial of coverage put it on notice that additional documentation supporting medical necessity was required.[13] In another case, the

10. *See Meridian Laboratory Corp. v. AdvanceMed Corp.* (PSC), Departmental Appeals Board, Decision of Medicare Appeals Council, 2011 WL 6960470 (June 24, 2011), remanded, 2012 WL 3112066 (W.D. N.C. 2012).
11. *Virtual Imaging Services v. First Coast Service Options,* Departmental Appeals Board Decision of Medicare Appeals Council, M-14-1254 (May 16, 2014).
12. *Maximum Comfort, Inc. v. Secretary*, 512 F. 3d 1081, 1088-89 (9th Cir. 2007).
13. *See D/B/A I.M.I.G. Sonomed Diagnostics,* Departmental Appeals Board, Decision of Medicare Appeals Council, 2013 WL 7217919 (March 7, 2013).

council did not even address application of potentially applicable limitation of liability principles, resulting in a federal court's remand of the case back to the council so that it could do so.[14]

Preventive Actions

Although clinical laboratories may view the medical necessity issue as Medicare's version of "blame the victim," there are some actions that a laboratory can take to protect itself from denial of Medicare claims based solely on the content of the physician's medical record or its lack of access to those records.

A laboratory can educate physicians regarding its need for a copy of the physician's medical records to support the medical necessity of clinical laboratory tests that the physician ordered.[15] If there is any type of contractual relationship with the physician or medical group, the laboratory might consider including a provision requiring the physician or medical group to provide medical record documentation upon the laboratory's request.

A laboratory can educate physicians regarding its need for a copy of the physician's medical records to support the medical necessity of clinical laboratory tests that the physician ordered.

A laboratory should encourage referring physicians to personally sign test requisitions. Although CMS has stated that this is not required by Medicare regulations, a signed requisition may eliminate risk of assertions that the test was not "ordered" (or that the laboratory did not provide documentation of the test order) or that the order was not authenticated as required by Medicare regulations.

A laboratory should also confirm that it is obtaining Advance Beneficiary Notices of Noncoverage (ABNs) whenever appropriate and is encouraging physicians to do so on its behalf when the individual for whom testing is to be performed does not personally present at a laboratory patient service center.[16]

Conclusion

Medical necessity requirements will continue to raise troublesome issues for laboratories. However, laboratories should take available actions to limit their financial exposure and should continue to argue based on limitation of liability principles in appropriate cases. After all, in doing so, they are asking only that these provisions be applied based on their stated terms, as Congress likely intended.

Robert E. Mazer is a shareholder in the Baltimore-based firm of Ober | Kaler where he concentrates on representation of hospitals, clinical laboratories and other providers of diagnostic services. He can be reached at *remazer@ober.com*.

14. *Meridian Laboratory,* 2012 WL 3112066.
15. Medicare regulations provide for CMS to request such documents from the ordering physician. If it does not receive the requested documents, the Medicare claim is denied. They also permit the laboratory to request such documents from the physician. 42 C.F.R. § 410.32(d)(2), (3). One MAC has indicated that a physician's failure to cooperate with a supplier violates a legal requirement. See n.3 and accompanying text..
16. The provision of an ABN, however, has been used as evidence that the provider had some knowledge that the services would be denied on medical necessity grounds. CMS forbids "routine ABNs" that state only that Medicare denial of payment "is possible"; according to the agency, an ABN must specify a "genuine reason that denial by Medicare is expected." CMS Medicare Claims Processing Manual, Ch. 30, *§ 40.3.6.1*. It is difficult to reconcile this manual provision with the agency's position that a Medicare provider may not invoke limitation of liability because it should be aware that Medicare payments may be denied if additional documentation required to establish medical necessity is requested, but not provided. See n. 12 and accompanying text.

    Close attention to ABN requirements is generally advisable. In one recent case, an administrative law judge ruled that an ABN that was provided to a patient after he arrived at a hospital for collection of his specimen was ineffective because it was a last-minute, coercive notice that did not permit the beneficiary to make a rational, informed consumer decision. *Appeal of Olympic Medical Center*, ALJ Appeal No. 1-1097162747 (Dec. 9, 2013), *appeal pending*, Medicare Appeals Council (2014). ABNs have also been rejected based on use of acronyms, because they were "equivocal" or because they did not provide a meaningful explanation of reasons why Medicare was likely to deny payment.

Medicare Provides Details on How to Bill for Hepatitis C Screening, *from page 1*

Both transmittals have effective dates of June 2 and implementation dates of Jan. 5, 2015, for nonshared Medicare administrative contractor edits and common working file analysis, and April 6, 2015, for the remaining shared system edits. This means that labs may not be able to depend on Medicare denials to detect claims that violate frequency or diagnosis code requirements on the effective date and must take action to avoid submitting inappropriate claims.

Transmittal R3036CP introduces a new Healthcare Common Procedure Coding System (HCPCS) code G0472, "Hepatitis C antibody screening for individual at high risk and other covered indication(s)" along with the necessary International Classification of Diseases, Ninth Revision (ICD-9) and International Classification of Diseases, Tenth Revision (ICD-10) codes that must accompany the new HCPCS code to avoid denials. It also provides the specific reason and remark codes that will be used with denials. The new information appears in the claims processing manual in sections 210 through 210.4.

CMS Exclusions May Cause Confusion

Under Medicare, HCV screening is covered for beneficiaries at high risk for an HCV infection. High risk means persons with a current or past history of illicit injection drug use and persons who have a history of receiving a blood transfusion prior to 1992. Screening tests for adults who do not meet the definition of high risk but were born between 1945 through 1965 are allowed once in a lifetime.

Annual screening is allowed for high-risk patients who have continued illicit injection drug use since the last negative screening test. Determination of high risk for HCV is made by the primary care physician and must be properly documented in the patient medical record. Once again, labs are at the mercy of physicians to order the HCV screening test only when appropriate and to properly document that service.

Hospitals and other institutional providers must use type of bill (TOB) codes 13X and 85X when billing with G0472. Note that TOB 14X for non-hospital patients is not included. For professional billing, only the following provided specialties are allowed:

01—General Practice	38—Geriatric Medicine
08—Family Practice	42—Certified Nurse Midwife
11—Internal Medicine	50—Nurse Practitioner
16—Obstetrics/Gynecology	89—Certified Clinical Nurse Specialist
37—Pediatric Medicine	97—Physician Assistant

Also, one of the following place of service (POS) codes is required on claims for G0472:

11—Physician's Office	49—Independent Clinic
22—Outpatient Hospital	71—State or Local Public Health Clinic

Note that independent labs, specialty code 69 and place of service code 81, are not included on either list. Since the majority of screening tests will be done and billed by independent labs, the industry should seek clarification.

Diagnosis Codes Required

For those beneficiaries determined to be high-risk, ICD-9 diagnosis code V69.8, (other problems related to lifestyle) is required on claims in addition to G0472. Once ICD-10 is implemented, labs should use diagnosis code Z72.89 (other problems related to lifestyle).

For annual coverage when appropriate, the same ICD diagnosis code V69.8/Z72.89 will be included along with ICD-9 code 304.91 (unspecified drug dependence, continuous) or ICD-10 code F19.20 (other psychoactive substance abuse, uncomplicated).

For annual screenings, 11 full months must pass following the month of the last negative HCV screening.

Reason and Remark Codes

There are different claim adjustment reason codes (CARCs) and remittance advice remark codes (RARCs) that will be included on claims when services are denied. It is important for lab billing employees to be aware of what these codes mean so they can take the appropriate corrective action in the case of a denial. For instance, for institutional claims that are denied for TOB, the following codes should be included with the denial notice:

- CARC 170—Payment is denied when performed/billed by this type of provider.
- RARC N95—This provider type/provider specialty may not bill this service.

The transmittal defines specific CARCs and RARCs for each specific denial for both institutional and professional claims. Medicare summary notice codes are also included in the transmittal.

Further Clarification Needed

Another issue not clear in either of the transmittals concerns what tests are being performed and whether their HCPCS codes should be included on the claims. Here is what transmittal R174NCD says about the tests that should be used: "CMS will cover screening for HCV with the appropriate U.S. Food and Drug Administration (FDA) approved/cleared laboratory tests, used consistent with FDA-approved labeling and in compliance with the Clinical Laboratory Improvement A[mendments] regulations." The original decision memorandum says the following, "Initial testing for HCV should be performed using the most sensitive immunoassays licensed for detection of antibody to HCV (anti-HCV) in blood." Further, there is no mention of reimbursement for G0472. This is another area where clarification is needed.

Actions Your Lab Should Take

The lab is dependent on the primary care physician to order the test correctly, and to document appropriately in their patient medical records.

The lab should make an educational contact with its customers concerning the requirements of the new benefit. Physicians should clearly identify the test as a hepatitis screening test and clearly indicate under which scenario the testing is being performed, either the once-in-a-lifetime or annual test. This will allow the lab to ensure the correct diagnosis information is included.

The laboratory should enter the new HCPCS code into their billing systems and include edits for the required diagnosis codes, TOB, specialties, and POS if their system allows. If not, you will need to develop some kind of manual process to make the determinations. If using a third-party billing company, make certain they include the codes and edits in their billing systems.

Since this is a screening test with a frequency limitation, the laboratory may collect advance beneficiary notices (ABN) on all Medicare patients. The communication should instruct ordering physicians to collect ABNs.

Labs should also contact their Medicare administrative contractor to seek clarification on the problem areas identified in this article. Document the call for future reference or to help with appeals and claims denials.

Phlebotomists, test entry employees, billing employees, and customer service employees should be educated about the new screening benefit and how to detect and report problems.

In addition, policies and procedures and annual compliance education and training material should be updated to help ensure compliance with the requirements of the new benefit.

Takeaway: There is a potential for an increased order volume for the new HCV screening benefit as Medicare beneficiaries become aware of it. Laboratories should become familiar with billing requirements to avoid potential compliance problems that may be associated with the screening.

One More Threat to Consider With a HIPAA Breach in Your Laboratory

An Illinois court recently granted a motion to dismiss a class-action lawsuit that resulted from a Health Information Portability and Accountability Act (HIPAA) breach of protected health information (PHI). The court ruled that plaintiffs cannot claim injuries based merely on potential losses.

The breach by Advocate Health and Hospitals Corp. in Downers Grove, Ill., occurred in August 2013. Because there is no private cause of action under HIPAA, the only course of action for the plaintiffs were state laws—in this case the Illinois Personal Information Protection Act and the Illinois Consumer Fraud Act and invasion of privacy.

The Case

The breach was one of the largest at that time and involved the theft of four unencrypted laptop computers from an Advocate medical group building that included the PHI of over 4 million patients. Advocate faced fines and sanctions under HIPAA and the class-action suit served to complicate their problem even more. Eventually, Advocate filed a motion to dismiss the lawsuit, saying that the plaintiffs had no standing and had not made a specific claim.

Advocate's motion was granted because the plaintiffs could not prove that the PHI had been viewed or used in any harmful way, therefore there was no proof of identity theft. The court ultimately agreed with Advocate's argument and dismissed the suit with prejudice.

Lessons for Laboratory Privacy and Compliance Officers

Compliance breaches can happen to anyone and there have been several that are specific to laboratories, such as the case reported elsewhere in this issue. Even though this case is not lab specific, it does raise awareness of the multiple legal risks that can result from a single breach.

Takeaway: Compliance threats from HIPAA breaches have grown in frequency and variety, which highlights the need for labs and other providers to ensure that all PHI is protected and secured.

Compliance Corner

There have been a number of anti-kickback and physician self-referral (Stark) cases involving laboratories this year. Many laboratory compliance officers are not sufficiently familiar with these laws and regulations to make good decisions when it comes to them. Here are a few tips that may be helpful when these laws are implicated.

If the anti-kickback laws are implicated, it is essential that any potential Stark implications are examined. Often, both are involved. One key element for Stark violation is that a physician or practitioner who can make referrals must be involved. Generally speaking—no physician, no Stark problem. These laws include more criteria than just the issues of fair market value and value and volume of referrals. Always examine all of the criteria for a safe harbor or a Stark exception.

When considering whether there is an anti-kickback violation, look for anything that ties or implies that remuneration is being given in consideration for, or in exchange for, referrals. Exclusivity clauses in any agreements or language that requires the referral of other business in order to receive the remuneration are red flags.

To ensure you are in compliance with Stark, if your lab is paying physicians for any service, providing something for free or giving them anything of value, you must find an exception for it, and all of the criteria for the exception must be met. For either of these laws, written agreements are required.

Finally, the consequences of violations of these laws are severe. If you are unsure that what you are being asked to approve is legal, seek the advice of counsel familiar with these laws and their application to the clinical laboratory setting.

News-At-A-Glance

DRUG TESTING LAB FORFEITS $753,955 TO GOVERNMENT: Federal prosecutors filed a motion to seize financial accounts belonging to Universal Oral Fluid Laboratories (UOFL) and its owner William Hughes in a case involving sham joint venture agreements with physicians that provided kickbacks for referrals to the lab. The Pennsylvania drug testing lab was seeking to be the exclusive lab for providing drug testing services nationwide. According to court documents, UOFL received $42 million from commercial insurances and $11.2 million from Medicare between January 2011 and November 2013. One physician who conspired with Hughes in the scheme accounted for approximately $1.9 million of the Medicare revenue deposited in one of the accounts. Hughes wrote checks to himself and his wife and moved money from one account to another. Since the money was gained through violations of federal law, the government has a right to seize it and did so. The investigation into UOFL is continuing.

LABORATORIES SEEN AS EMBRACING PATIENT DIRECT ACCESS TO TEST RESULTS: In a Sept. 15 story, the *Wall Street Journal* says that patient access to laboratory test results is a good thing and that labs are providing tools and information to help patients understand their test results. Effective Oct. 6, labs are required to provide direct access to a patient's test results within 30 days after the test is finalized. Initially, labs viewed the 30-day window as an opportunity to allow physicians to review sensitive test results with patients before the patient sees the test results themselves. Ideally, this is fine, but labs may be ignoring facts gleaned from a 2009 study that says patients do not receive notice of abnormal test results for one in every 14 tests. Many labs have already started providing test results, including the two largest labs in the country. According to the article, some labs are creating special test reports designed to help patients interpret the information in the result. Labs that do not embrace this trend and resist providing meaningful information for patients may be missing an opportunity to get recognized for the value their tests contribute to the health care system and patient care.

PROTECTING MEDICARE FROM FRAUD: Draft legislation on protecting Medicare from fraud has implications for the laboratory industry. House Ways and Means Subcommittee on Health Chairman Kevin Brady (R-Texas) recently released a draft of the bill titled Protecting Integrity in Medicare Act of 2014. Among the provisions that may affect labs include removing Social Security numbers from Medicare cards, reducing improper payments through education and the provision of specific data to a provider concerning erroneous payments, additional funding for the Health and Human Services inspector general, expansion of the Senior Medicare Patrol program to cover Medicaid and provide more incentives for seniors to participate, and alternative predetermined sanctions for technical violations of the Stark self-referral laws if voluntarily disclosed. Laboratory providers need not take any action other than commenting on the legislation at this time but should monitor the progress of this legislation.

 G2 Compliance Advisor (ISSN 2332-1474) is published by G2 Intelligence, 24 Railroad Street, Keene, NH 03431-3744 USA. Tel: 800-531-1026 or +1-603-357-8101. Fax: +1-603-357-8111. Web site: www.G2Intelligence.com.

Kimberly Scott, Managing Editor, kscott@G2Intelligence.com; Christopher Young, Editor; Heather Lancey, Designer; Beth Butler, Marketing Director; Dan Houder, President and Publisher