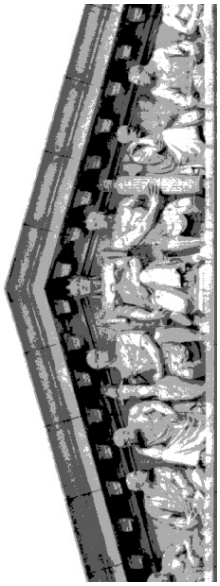
G-2 Compliance Report

WASHINGTON G-2 REPORTS

Vol. X, No. 10, Nov.-Dec. 2008

For Hospitals, Laboratories and Physician Practices



Kimberly Scott, Senior Editor,
kscott@ioma.com

Inside this issue

www.g2reports.com

FDA Warns LabCorp About OvaSure Claims

The Food and Drug Administration (FDA) warned LabCorp that it is marketing the company's OvaSure ovarian cancer test in violation of the law.

In a warning letter dated September 29, Steven Gutman, director of the FDA's Office of In Vitro Diagnostic Device Evaluation and Safety, warned LabCorp President and CEO David King that an FDA review had "revealed serious regulatory problems" with the test.

Specifically, the FDA has determined that "OvaSure is a test that was designed, developed, and validated by investigators at Yale University and not LabCorp." As such, the test is not a lab-developed test, which does not require FDA approval.

Because LabCorp did not obtain marketing approval or clearance from the FDA for the OvaSure test, marketing the test is a violation of the law, writes Gutman, who advises the company to take prompt action to correct the violation. Failure to correct the violation may result in regulatory action being initiated by the FDA without further notice. The actions include, but are not limited to, seizure, injunction, and civil monetary penalties.

OvaSure is intended to identify high-risk women who might have ovarian carcinoma, but FDA officials have taken issue with promotional claims that the test has 95.3 percent sensitivity and 99.4 percent specificity.

Eric Lindblom, LabCorp's senior vice president of investor and media relations, tells G-2 Reports that the company is in discussions with the FDA over the most appropriate next steps. LabCorp hopes to work with the FDA to address these regulatory issues, he says.

OIG Sets Focus Areas for 2009

The Health and Human Services Office of Inspector General (OIG) plans to continue its review of inappropriate unbundling of clinical laboratory testing in the coming year, the agency says in its fiscal 2009 work plan, published October 1.

Medicare requires that its contractors group together individual laboratory tests that clinical laboratories can perform at the same time on the same equipment and then consider the price of related profile tests. Payment for individual tests must not exceed the lower of the profile price or the total price of all the individual tests. The OIG plans to determine whether clinical

Continued on page 2

The OIG's 2009 work plan is available online at www.oig.hhs.gov/publications/docs/workplan/2009/WorkPlanFY2009.pdf

OIG Sets Focus Areas, *from page 1*

laboratories have unbundled profile or panel tests by submitting claims for multiple dates of service or by drawing specimens on sequential days. Reviewers will also determine the extent to which the Medicare carriers have controls in place to detect and prevent inappropriate payments for laboratory tests.

This is just one of the hundreds of areas targeted for review in 2009. The work plan, released each year, serves as a road map for what the OIG plans to target in the coming year.

The OIG also plans to review the extent of variation in laboratory test payment rates among Medicare contractors. The work plan notes that in 2007, Medicare payments for laboratory services exceeded $6 billion. Prior OIG work found that Medicare had paid significantly higher prices than other payers for certain laboratory tests. The agency in 2009 plans to analyze claims to determine pricing variances among Medicare contractors for the most commonly performed tests.

Medicare Billings With Modifier GY

Modifier GY is used for coding services that are statutorily excluded or do not meet the definition of a covered service. Providers are required to supply beneficiaries with advance notice of charges for services that are excluded from Medicare by statute. In fiscal 2006, Medicare received more than 53 million claims with a modifier GY and denied claims totaling over $400 million. The agency plans to examine patterns and trends for physicians' and suppliers' use of modifier GY.

The OIG also plans to review the extent of variation in laboratory test payment rates among Medicare contractors.

Separately Payable Lab Services Under ESRD

The OIG will review providers' compliance with the current payment policies for automated multichannel chemistry tests (AMCC) tests furnished to end stage renal disease (ESRD) beneficiaries. The Medicare Modernization Act (MMA) requires HHS to develop a report on a bundled prospective payment system for ESRD services. A bundled PPS could include certain lab tests that are currently separately billable.

The current facility payment, the composite rate, includes payments for certain AMCC tests provided routinely at specified frequencies. Any AMCC tests performed in excess of those frequencies or not included in the composite rate payment are to be paid separately, provided that medical necessity is documented.

To ensure that the bundled PPS rate is based on valid data, the OIG will review providers' compliance with the current payment policies for AMCC tests furnished to ESRD beneficiaries. It will also identify separately billed clinical lab tests that are regularly provided to ESRD beneficiaries in addition to the tests included in the composite rate.

Recovery Audit Contractors

The OIG will review CMS's oversight and monitoring of recovery audit contractors (RAC) to determine whether they meet contractual requirements outlined in the RAC Task Orders. The RAC program, authorized by the MMA, is designed to reduce improper Medicare payments through the detection and collection of overpayments, the identification of underpayments, and the implementation of actions that will prevent future improper payments.

Medicaid Payments for Dual-Eligible Beneficiaries

Medicare will reimburse 100 percent of allowable laboratory-service charges for beneficiaries who are enrolled in both Medicare and Medicaid. Because Medicaid is the payer of last resort, Medicaid should not pay any portion of charges for lab services provided to dual-eligible beneficiaries unless the services are provided in a hospital or rural health clinic. The OIG will determine whether selected state Medicaid programs made improper payments for outpatient laboratory services provided to dual eligibles in fiscal 2005.

CMS to Boost Fraud-Fighting Efforts

The Centers for Medicare and Medicaid Services (CMS) in October announced what it says are "aggressive new steps" to find and prevent waste, fraud, and abuse in Medicare.

As part of these steps, CMS is consolidating its efforts with new program integrity contractors that will look at billing trends and patterns across Medicare. They will focus on companies and individuals whose billings for Medicare services are higher than the majority of providers and suppliers in the community. CMS is also shifting its traditional approach to fighting fraud by working directly with beneficiaries by ensuring they receive the services for which Medicare was billed and that the items or services were medically necessary.

CMS also will be conducting more stringent reviews of payments to suppliers of durable medical equipment, prosthetics, and orthotics (DMEPOS). For those claims not reviewed before payment is made, CMS is implementing further medical review of submitted claims by one of the new recovery audit contractors (RACs).

Finally, CMS is consolidating the work of Medicare's program safeguard contractors (PSCs) and the Medicare Drug Integrity Contractors (MEDICs) with new Zone Program Integrity Contractors (ZPICs). The new contractors will eventually be responsible for ensuring the integrity of all Medicare-related claims under Part A and B, Part C, Part D, and coordination of Medicare-Medicaid data matches.

The first two ZPIC contracts were awarded to Health Integrity, LLC, for Zone 4 (Texas, New Mexico, Colorado, and Oklahoma) and Safeguard Services LLC for Zone 7 (Florida, Puerto Rico, and the U.S. Virgin Islands).

New Recovery Audit Contractors Named

The Centers for Medicare and Medicaid Services (CMS) has selected four new Recovery Audit Contractors (RACs), whose job it is to identify improper Medicare payments.

The new RACs are:

- **Diversified Collection Services Inc.,** Livermore, Calif., in Region A, initially working in Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, and New York.
- **CGI Technologies and Solutions Inc.,** Fairfax, Va., in Region B, initially working in Michigan, Indiana, and Minnesota.
- **Connolly Consulting Associates Inc.,** Wilton, Conn., in Region C, initially working in South Carolina, Florida, Colorado, and New Mexico.
- **HealthDataInsights Inc.,** Las Vegas, Nev., in Region D, initially working in Montana, Wyoming, North Dakota, Utah, and Arizona.

Additional states will be added to each RAC region in 2009. The RACs will be paid on a contingency fee basis on both the overpayments and underpayments they find.

The RAC program is mandated by law and is required to be in place by Jan. 1, 2010. The national program is an outgrowth of a demonstration program that used RACs to identify Medicare overpayments and underpayments to health care providers and suppliers in California, Florida, New York, Massachusetts, South Carolina, and Arizona. The demonstration resulted in more than $900 million in overpayments being returned to the Medicare Trust Fund between 2005 and 2008 and nearly $38 million in underpayments returned to health care providers.

As part of preparing providers for the RAC program as it is phased in nationally, CMS will continue working closely with national and state medical associations. Before work begins, the RACs will hold Town Hall type meetings in each state with health care providers and CMS staff. Providers can get more information about the meetings by checking the CMS RAC Web site at *www.cms.hhs.gov/RAC*.

Soon after outreach efforts are made, some health care providers in the states that are part of the first phase may begin to receive either requests for medical records or a letter requesting that an overpayment be repaid for their claims that were submitted to and paid for by Medicare. To prepare for the start of the program, health care providers should consider conducting an internal assessment to ensure that submitted claims meet the Medicare rules. Other steps providers should take include:

- Identifying where improper payments have been persistent by reviewing the RAC's Web sites and identifying any patterns of denied claims within their own practice or facility;
- Implementing procedures to promptly respond to RAC requests for medical records;
- Filing an appeal before the 120-day deadline if the provider disagrees with the RAC determination;
- Keeping track of denied claims and correcting these previous errors; and
- Determining what corrective actions need to be taken to ensure compliance with Medicare's requirements and to avoid submitting incorrect claims in the future.

Providers Question Timing of Conversion to ICD-10

A rule by the federal government requiring all hospitals to switch to a new health care coding system by 2011 would dramatically increase costs for physician practices and clinical laboratories, according to a study released October 14 by a group of provider organizations. The groups called on the Centers for Medicaid and Medicare Services (CMS) to reassess the implementation time frame.

According to a statement issued with the study, the costs associated with moving from the *International Classification of Diseases, Ninth Revision* (ICD-9) to the *International Classification of Diseases, Tenth Revision* (ICD-10) in such a short time are "markedly higher than what CMS has estimated and will place a major burden on providers, taking valuable time away from their patients and straining other resources needed to invest in health information technology."

The changes would mean that providers would go from having 17,000 procedure and diagnoses codes in ICD-9 to more than 155,000 such codes in ICD-10. When the preliminary rule was released, CMS said the expanded number of codes would accommodate new procedures and diagnoses and better enable implementation of electronic health records because of the greater level of detail that would be available in electronic transactions about procedures and diagnoses via ICD-10.

During a conference call for national providers about the switch held the same day the study was released, CMS discussed the differences between ICD-9 and ICD-10 and explained that no final decision on the proposed implementation date has been reached.

According to the study, the total estimated cost for a 10-physician practice to move to ICD-10 would be more than $285,000. For a small, three-physician practice, the study found the total cost would be $83,290. For a large, 100-physician practice, the estimated costs would be more than $2.7 million.

The study was conducted by Nachimson Advisors and co-commissioned by a number of health care groups, including the American Clinical Laboratory Association. To view the study findings, go to http://nachimsonadvisors.com/products.aspx. The proposed ICD-10 rule is available at http://edocket.access.gpo.gov/2008/pdf/E8-19298.pdf.

COMPLIANCE PERSPECTIVES

Red Flags Rules: Identity Theft Protections Now Extend to Health Care Providers

Judith Waltz

Jennifer Karron

Andrew Serwin

Judith Waltz, Jennifer Karron, and Andrew Serwin are health care attorneys with Foley & Lardner LLP

Hospitals, clinical laboratories, and other medical care providers may be dangerously unaware that they have a looming deadline for compliance with complex new federal regulations.

These "Red Flags Rules" require the adoption and implementation of a broad identity theft prevention system by Nov. 1, 2008.

Neither the statute nor the implementing regulation issued by the Federal Trade Commission (FTC) expressly states its applicability to health care providers. However, the preamble to the regulations specifically discusses "medical identity theft," making it clear that the governmental entities responsible for enforcing these new provisions (and prosecuting cases of medical identity theft) will expect health care providers to exercise due diligence to conform with the new provisions.

For the health care provider, identity theft may result in unpaid claims, assessments of overpayments, or even allegations that false claims have been submitted.

Medical Identity Theft a Growing Concern

Medical identity theft may occur for purposes of obtaining medical items (including drugs) or services or for purposes of fraudulently obtaining money relating to medical items or services.

As defined by the Department of Health and Human Services (HHS) on its Web site, medical identity theft is a "specific type of identity theft which occurs when a person uses someone else's personal health identifiable information, such as insurance information, Social Security Number, health care file, or medical records, without the individual's knowledge or consent to obtain medical goods or services, or to submit false claims for medical services."

In May 2008, HHS's Office of the National Coordinator for Health Information Technology (ONC) awarded a $450,000 contract to Booz Allen Hamilton to assess and evaluate the scope of the medical identity theft problem in the United States. Its final report is expected to be released sometime during the next six months (late 2008 or early 2009) and will set forth possible next steps for the federal government and other stakeholders to work toward prevention, detection, and remediation of medical identity theft.

Even the federal government is not immune from current scrutiny with respect to its efforts to avoid medical identity theft. HHS's Office of Inspector General indicated in its annual 2009 Work Plan that it will review the efforts of the Centers for Medicare and Medicaid Services (CMS) to deter medical identity theft, including its outreach to beneficiaries.

Medical identity theft may result in insurance claims for items or services that have never been provided, were provided to

different individuals than those whose insurance is billed, or that are billed in exaggerated amounts. Health care plans are obvious targets.

For the health care provider, these scenarios may result in unpaid claims, assessments of overpayments, or even allegations that false claims have been submitted. For the individual whose identity is stolen, there may be credit collection attempts against them for services they never received, as well as consequences for their ongoing health insurance coverage such as higher premiums or even cancellation if maximum benefits are reached.

Perhaps of most concern for individuals is the possibility of inaccurate medical records, which may have adverse clinical implications for ongoing health care. Resolving these medical record inaccuracies in all the multiple places where an individual's medical records are now kept could well become a lifetime pursuit. For society, the costs of medical identity theft may include higher insurance costs, inappropriate use of government programs (including government-provided health insurance as well as costs associated with investigation and enforcement), and an inappropriate distribution of health care resources.

Overview of the Red Flags Rules

In short, the new Red Flags Rules apply to those who are defined as "creditors," which, as discussed below, can include health care entities. These entities are expected to take proactive steps after having identified their "red flags" ("risk areas" to use terminology more familiar in the world of health care compliance), to put in place measures that will minimize the risk of identity theft, and to respond when the red flags suggest an attempt at theft. Involvement by the board of directors (or functional equivalent as defined) is required to approve the plan of action.

Perhaps of most concern for individuals is the possibility of inaccurate medical records, which may have adverse clinical implications for ongoing health care.

'Creditor' Defined

For purposes of the Red Flags Rules, a creditor is defined as "any person or business who arranges for the extension, renewal, or continuation of credit" with a "covered account." An account is defined as a continuing relationship with a creditor to obtain a product or service and includes deferred payments for services or property. A covered account is: 1) an account primarily for personal, family, and household purposes that involves or is designed to permit multiple payments or transactions; and 2) any other account (including an account for business purposes) for which there is a reasonably foreseeable risk to customers or the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

Health care providers may have accounts that satisfy these definitions in various ways. Most health care providers extend credit to at least some patients by offering them extended payment plans. Some may also extend credit to employees or to other parties.

In California, Medi-Cal (the state's Medicaid program) may permit "share of cost" obligations to be paid over time. Each health care provider should, as a first step, think through what types of transactions it offers in the course of business that would meet the definition of a "covered account."

What Types of Activities Could Be Red Flags?

Individual entities must conduct their own self-scrutiny to determine what types of behavior or events they may have experienced (or to which they may be susceptible) that

would suggest the potential for medical identity theft. Possibilities may include situations involving the exhaustion of lifetime benefit limits, denials for duplicate or excessive services for one individual, identified fraudulent reimbursement or insurance submissions, or discrepancies in information collected at the time of providing services.

Some provisions of HIPAA may be implicated in the event of actual, suspected, or attempted medical identity theft.

Patient and insurer complaints about bills for items or services never received should be taken very seriously, even though many such complaints turn out to be without merit due to understandable patient confusion about their bills or about the multiplicity of providers of services involved in their care. To properly define and implement their Red Flags program, health care organizations must learn lessons from others, keeping abreast of the identity theft environment and tapping sources such as literature and information from credit bureaus, financial institutions, other creditors, designers of fraud detection software, and from their own prior experience.

Red Flags Rules Require More Than HIPAA Compliance

While all health care providers are used to the privacy and security rules applicable under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), these new provisions are likely to require some enhanced steps with respects to covered accounts, as defined above. Obviously, some HIPAA-protected information might serve as a basis for medical identity theft.

In addition, though, the health care provider must consider what other identifying information it might have in its possession which, even if arguably not protected health information, might be used for improper purposes leading to a possibility of medical identity theft.

Identifying information means any name or number that may be used alone or in conjunction with any other information to identify a specific person, including: Social Security number; date of birth; official state- or government-issued driver's license or identification number; passport number; alien registration number; unique biometric data; unique electronic identification number, address, or routing code; or telecommunication identifying information or address device and so forth.

Thus, under the Red Flags Rules, the creation of a fictitious identity using any single piece of information belonging to a real person falls within the definition of identity theft.

Some provisions of HIPAA may be implicated in the event of actual, suspected, or attempted medical identity theft. These include HIPAA's provisions that a patient should have an opportunity to correct false information in his or her records and that a patient may request an accounting of what information has been disclosed, to whom it was disclosed, and why it was disclosed. Both provisions have limitations that presumably are addressed in the health care provider's HIPAA compliance program, which may merit a second look in light of the Red Flags Rules.

Genesis of the Red Flags Rules

The 2003 Fair and Accurate Credit Transactions Act (FACT Act), which created these Red Flags Rules, was one of the first federal financial privacy laws that applied to nonfinancial institutions. As new rules implementing the FACT Act have been implemented, the burdens placed upon nonfinancial institutions have only grown and recently enacted rules have added to the burdens placed upon companies, whether they are financial institutions or not.

The new provisions actually became effective on Jan. 1, 2008, although there is a phased-in compliance date of Nov. 1, 2008.

What to Do to Meet the New Requirements

At a minimum, health care entities should take the following steps to strive for compliance with the Red Flags Rules:

1. Periodically identify covered accounts. Each creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, the creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts, taking into consideration:

- The methods it provides to open its accounts;
- The methods it provides to access its accounts; and
- Its previous experiences with identity theft.

2. Establish an Identity Theft Prevention Program. Creditors that offer or maintain one or more covered accounts must develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The program must be appropriate to the size and complexity of the creditor and the nature and scope of its activities. The program must include reasonable policies and procedures to:

- Identify relevant Red Flags for the covered accounts that the creditor offers or maintains and incorporate those Red Flags into its program;
- Detect Red Flags that have been incorporated into the program of the creditor;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
- Ensure the program (including the Red Flags determined to be relevant) is updated periodically to reflect changes in risks to customers (i.e., a person that has a covered account with a financial institution or creditor) and to the safety and soundness of the creditor from identity theft.

3. Administer the Red Flags Program. Creditors, if required to implement a Red Flags Program, must also provide for the continued administration of the program and must:

- Obtain approval of the initial written program from either its board of directors (or functional equivalent, as defined) or an appropriate committee of the board of directors;
- Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation, and administration of the program;
- Train staff, as necessary, to effectively implement the program; and
- Exercise appropriate and effective oversight of service provider (i.e., a person that provides a service directly to the financial institution or creditor) arrangements.

4. Consider any pertinent state laws that may be implicated by your Red Flags Program.

Conclusion

The Red Flags Rules impose significant new challenges for health care providers, with a short time for turnaround. Even health care providers with robust compliance programs should review what protections are in place to protect against medical identity theft and assure that it knows what its "red flags" might be.

- *Judith Waltz can be reached at 415-438-6412, jwaltz@foley.com; Jennifer Karron can be reached at 414-297-5610, jkarron@foley.com; and Andrew Serwin can be reached at 619-685-6428, aserwin@foley.com.*

Cardiologists Say CMS Overstepped on Stark Changes

A group of cardiologists in Colorado has filed a federal complaint against Health and Human Services Secretary Michael O. Leavitt, saying the Centers for Medicare and Medicaid Services (CMS) overstepped its authority in making a recent change to the physician self-referral rules (*Colorado Heart Institute v. Leavitt*).

The change effectively would put the doctors' cardiac catheterization labs out of business, according to the complaint, because it would cause Medicare business generated through contracts with local hospitals to dry up.

At issue is CMS's expanded definition of "entity" and how the change would affect so-called "under arrangements" in which physician groups contract with hospitals to provide services on behalf of the hospitals at physician-owned outpatient facilities.

The change was made in the fiscal year 2009 hospital inpatient prospective payment system rule (IPPS), published August 19. In that rule, CMS expanded the definition of an "entity" for Stark rule purposes to include providers that perform designated health services (DHS), as well as providers that are paid directly by Medicare for the services. Historically, only providers that are paid directly by Medicare for services were considered DHS entities under Stark.

The change effectively would put the doctors' cardiac catheterization labs out of business, according to the complaint.

The change was aimed particularly at curbing certain joint ventures for services provided "under arrangements" by physician organizations on behalf of hospitals that bill the Medicare program for those services.

However, the cardiologists argued in the complaint that CMS "impermissibly" redefined DHS entities in the IPPS rule because Congress wrote into the Stark law an under arrangement exception that expressly allows similar contractual agreements as long as they meet certain requirements. Instead, the complaint continued, CMS's revised definition "impermissibly voids the statutory compensation exception by requiring qualifying arrangements to meet an ownership exception."

Under Arrangement Exceptions

Before the recent change (the provision actually becomes effective Oct. 1, 2009), under arrangement agreements between physician groups and hospitals were considered compensation arrangements only for the purpose of physician self-referral rules, commonly referred to as Stark rules. As such, CMS required that the deals meet at least one compensation exception under the Stark law.

The new definition of entity under Stark, however, would mean that physicians also must meet an ownership exception to continue referring patients for Medicare-covered services performed at their cardiac cath labs.

Providers that are considered DHS entities must meet an ownership exception under Stark to refer patients to those facilities because the law prohibits physicians from referring patients to a DHS entity for Medicare-covered services if they have an ownership interest.

In the case of the cardiac cath lab that brought the complaint, the referring physicians have ownership in the labs where the Medicare-covered services are performed.

Before the IPPS rule, physicians could refer patients for services performed at the labs in which they had ownership interest because the labs did not meet the definition of a DHS entity, but, beginning in October 2009, such referrals no longer can be made unless they meet an ownership exception (such as for rural owner-

ship) because the physicians' ownership interest will be considered to be in DHS entities.

Billing Limits

According to the complaint, a large majority of the cardiac procedures performed under arrangements between the physician groups and hospitals can be billed to Medicare only if performed in a hospital setting, meaning the cath labs must contract with hospitals to perform the procedures for Medicare patients. Services performed under arrangements are billed to Medicare by the hospitals, not by the physician organizations.

That would mean that the services currently provided under arrangements by the plaintiffs, and other providers in similar contracts with hospitals, could only be performed by hospitals, not by their contractors. For the cath labs that brought the complaint, 94 percent of the services they perform for Medicare patients must be billed by the hospital, meaning they would be left with too little business to stay open.

While CMS has said that under arrangement deals raised concerns about risks of overutilization of services, the cardiologists argued in the complaint that the arrangements are beneficial to hospitals because the cath labs owned and operated by physicians can perform heart procedures more efficiently and at a savings to the Medicare program.

Court Rejects Theory That Turns Medicare Rule Violations Into FCA Suits

A federal appeals court October 2 dismissed a lawsuit after finding no basis in either law or logic to adopt an express false certification theory that turns every violation of a Medicare regulation into the subject of a False Claims Act qui tam action (*United States ex rel. Conner v. Salina Regional Health Center Inc.*).

The U.S. Court of Appeals for the Tenth Circuit upheld a district court's decision finding that ophthalmologist Brian E. Conner cited no regulations or case law indicating that the government normally seeks retroactive recovery of Medicare payments for services actually performed on the basis that the noncompliance rendered them fraudulent.

The appeals court rejected Conner's argument that the certification of compliance in the Medicare cost report submitted by Salina Regional Health Center Inc., in Salina, Kan., standing alone, explicitly conditions Medicare payments on compliance with all applicable Medicare statutes and regulations.

"[T]he certification in the annual cost report represents the provider's assurance that it continues to comply with the requirements of Medicare participation. Implied in this certification is the recognition that the provider could face consequences through the administrative procedures . . . if it falls short of substantial compliance," Judge Carlos F. Lucero wrote.

"Based on the fact that the government has established a detailed administrative mechanism for managing Medicare participation, we are compelled to conclude that although the government considers substantial compliance a condition of ongoing Medicare participation, it does not require perfect compliance as an absolute condition to receiving Medicare payments for services rendered," Lucero added.

Perfect Compliance

James F. Segroves, an attorney with Proskauer Rose LLP, Washington, says the concept that substantial compliance does not require perfect compliance has been recognized at the district-court level before, particularly in cases involving nursing facilities, but never at the court-of-appeals level and not in the hospital context.

"[This case] is the first time that a federal court of appeals has recognized in a FCA case that the federal government doesn't expect 100 percent compliance with Medicare conditions of participation," Segroves said. "In other words, Congress and [the Centers for Medicare & Medicaid Services] have established an administrative process to take care of periodic noncompliance (which is expected to occur from time to time), and the FCA shouldn't be used as a vehicle to supplant that process."

Conner worked as a member of the medical staff at Salina for 18 years. Eventually, Conner developed a contentious relationship with the hospital in which Salina administrators challenged Conner's practices in the operating room and his treatment of hospital scrub staff.

"[This case] is the first time that a federal court of appeals has recognized in a FCA case that the federal government doesn't expect 100 percent compliance with Medicare conditions of participation."
—James F. Segroves

In turn, Conner complained that the hospital hired underqualified scrub staff, provided inadequate facilities and equipment, failed to meet required standards of care, and failed to investigate or review complaints concerning quality-of-care issues.

In 1995, Salina suspended Conner's privileges to perform certain ophthalmic procedures at its facilities. In May 1996, the hospital's chief executive officer notified Conner that the hospital would restore Conner's privileges if Conner agreed to contract with preferred scrub staff if the hospital's staff did not meet his needs and to work with Salina's surgery department to provide additional training to the hospital's scrub staff.

Reappointment Declined

Conner refused to sign the cooperation agreement and the hospital refused to lift his suspension, but Conner continued to perform other types of surgery until early 1997, when Salina declined to reappoint him to its medical staff.

When Conner filed the FCA qui tam action in the U.S. District Court for the District of Kansas, the district court ruled that Conner failed to state a claim under the FCA for Salina's alleged failure to comply with Medicare statutes and regulations because the government's payment for services rendered was not conditioned on such compliance.

The district court also dismissed Conner's claim under the anti-kickback statute, concluding that Conner's complaint failed to allege that the hospital had solicited a kickback in return for Medicare referrals. The district court also dismissed without prejudice Conner's state law claims of breach of contract and tortuous interference.

On appeal, the Tenth Circuit also dismissed Conner's assertion that Salina violated the FCA by submitting claims while failing to comply with the Medicare anti-kickback statute. The appeals court determined that Conner did not allege a kickback within the meaning of the anti-kickback statute, finding his refusal to use allegedly sub-par staff and Salina's attempt to accommodate the refusal did not amount to a kickback.

In addition, the appeals court found that Salina's letters to Conner, discussing conditions under which Conner's appointment would be renewed, did not address his ability to receive Medicare referrals. Finally, the appeals court found that the district court should have dismissed the state claims with prejudice. The Tenth Circuit found that Conner's state law claims were barred by the statute of limitations because the refiling period had run when he first served Salina.

The appeals court affirmed the district court's dismissal of Conner's FCA claims. However, the appeals court vacated the dismissal of Conner's state law claims without prejudice and remanded with instructions to dismiss the claims with prejudice.

Compliance Program Guidance: The Health and Human Services Office of Inspector General (OIG) has published new voluntary supplemental compliance guidance for nursing facilities. The guidance responds to developments in the nursing facility industry, including changes in the way facilities deliver and receive reimbursement for health care services, evolving business practices, and changes in the federal enforcement environment. A significant goal of the guidance is fostering quality of care in facilities. As such, it is designed to help compliance professionals address areas such as staffing, resident care plans, medication management, appropriate use of psychotropic medications, and resident safety. The guidance is available at *www.oig.hhs.gov/fraud/docs/complianceguidance/nhg_fr.pdf*.

Clinic Guilty of Fraud: A North-Carolina based clinic and its president have pleaded guilty to federal charges of fraudulently billing public and private health insurers. According to federal prosecutors, Kannapolis, N.C.-based Cannon Family Medicine Inc. and Christopher Caggiano, the clinic's president, pleaded guilty to four counts of health care fraud October 8. The defendants allegedly submitted $600,000 in fraudulent claims for allergy-testing services never performed. The insurers also were billed for echocardiograms and diagnostic ultrasounds even though the providers did not prepare written interpretations of the evaluations. Each of the four counts carry a maximum penalty of 10 years in prison and a fine of up to $250,000. Sentencing is set for Feb. 11, 2009.

New Part D Guidance: The Centers for Medicare and Medicaid Services (CMS) has issued new guidance to health insurers to clarify provisions in the recent Part D and Medicare Advantage marketing regulations affecting sales activities for the 2009 benefit year. In an October 8 memo to plan sponsors, CMS's Center for Drug and Health Plan Choice Director Abby Block said the guidance was in response to numerous questions about how to implement the rules, especially new requirements on compensating marketing and sales agents for enrolling beneficiaries in Part D and MA products. CMS had delayed implementation of the compensation provisions until October 8; Block extended that deadline to October 15.

 G-2 Compliance Report (ISSN 1524-0304) is published by Washington G-2 Reports, 1 Washington Park, Suite 1300, Newark, NJ 07102-3130. Tel: 973-718-4700. Fax: 973-622-0595. Order line: 212-629-3679. Web site: www.g2reports.com.

Kimberly Scott, Senior Editor; Dennis Weissman, Executive Editor; Janice Prescott, Sr. Production Editor; Perry Patterson, Vice President and Publisher; Joe Bremner, President.

Receiving duplicate issues? Have a billing question? Need to have your renewal dates coordinated? We'd be glad to help you. Call customer service at 973-718-4700.