G-2 Compliance Report

WASHINGTON G-2 REPORTS

Vol. II, No. 6, June-July 2001

For Hospitals, Laboratories and Physician Practices

Expect No Letup In Federal Fraud Pursuit

If you thought the government was easing up on scrutiny of hospitals, laboratories, and physicians, think again.

As several recent settlements indicate, the Department of Justice (DOJ) is actively cracking down on what it views as fraudulent billing practices by healthcare providers.

The increase in fraud probes actually began several years ago with passage of legislation guaranteeing federal agencies a cut of any money recovered, according to Judy Waltz, a partner with the law firm of Foley & Lardner (Washington, DC) and co-chair of the firm's corporate compliance practice for healthcare providers. For example, 3% of recoveries are allotted to the Health Care Fraud & Abuse Control Account established for use by DOJ and the Department of Health & Human Services. In 2000, $158 million was allotted to the account.

While the scrutiny is not new, investigators seem less forgiving when it comes to billing errors, notes Waltz. With advances in technology, for example, federal investigators are better able to catch systematic billing problems and less likely to go easy when problems are caused by software glitches.

"I advise my clients that they need to look at what comes out of their computer system, not just what goes in," Waltz explains. "Providers need to be doing self-audits and looking

Continued on p. 2

Inside this issue

OIG, GAO Issue Warning On Consultants

The practices of some business consultants could land providers of healthcare services in hot water, warn two government agencies which urge providers to be vigilant and exercise good judgment when selecting and relying on consultants.

Advice given by some unscrupulous consultants could result in violations of both civil and criminal statutes, says a new report from the General Accounting Office. The GAO report, released during a June 27 hearing before the Senate Finance Committee, describes two workshops on billing and compliance issues in which advice was provided that is inconsistent with guidance from the HHS Office of Inspector General (OIG).

"Specifically, certain consultants advocated not reporting or refunding overpayments received from insurance carriers after they were discovered," the report notes. "The consultants also encouraged the performance of tests and procedures that were not medically necessary to generate documentation in support of bills for evaluation and management services at a higher level of complexity than actually confronted during patients' office visits."

OIG Weighs In

A Special Advisory Bulletin from the OIG, also released during the June 27 hearing, highlights specific consultant practices that should

Continued on p. 4

Strategies For Integrating HIPAA Standards Into Your Compliance Program

This is part one of a two-part article. Watch for more strategies and tips in the August issue.

Overwhelmed by the thought of developing a HIPAA compliance program?

While the task can be daunting, healthcare providers should begin taking systematic steps to integrate requirements of the Health Insurance Portability & Accountability Act (HIPAA) into their existing compliance programs, says Carrie King, chief compliance officer for the University of Texas M.D. Anderson Cancer Center in Houston.

Providers should start by assessing the needs of their institution or organization, determining the critical players, and constructing an action plan with timelines, says King. "It doesn't have to be detailed initially. You're going to have to do this in pieces and bites, then you can branch out and get it more detailed."

HIPAA should fit in naturally with your organization's existing compliance structure if you take advantage of current structures and players, believes King (*see sample organizational chart on p. 3*). For example, in a small facility, the chief financial officer could double as the privacy officer while a larger facility may want to hire a full-time staff person to handle privacy functions, she advises.

HIPAA committees should also be integrated with existing compliance committees, adds King. M.D. Anderson has formed a Privacy Subcommittee and Security Subcommittee, both of which fall under the auspices of the facility's Institutional Compliance Committee. Each subcommittee has its own workgroups.

While upper management should be involved in the HIPAA compliance committees, they should not constitute the sole membership, King says. "It's important to have a broad cross-section of staff on the HIPAA committees. You need people who know where your 'bombs' are, people who are on the front line."

HIPAA compliance requirements should also be integrated into each facility's general compliance education program, advises King. At M.D. Anderson, for example, new standards regarding privacy are incorporated into new employee orientation as well as into specialized training for various departments, such as the business and procurement offices.

"You can't do it just once a year, then forget about it," she explains.

Fraud Pursuit, *from page 1*

at what comes back from Medicare and other payers in terms of denials, so they can identify problems early on. The government expects you to take a certain amount of care to be sure your bills are correct."

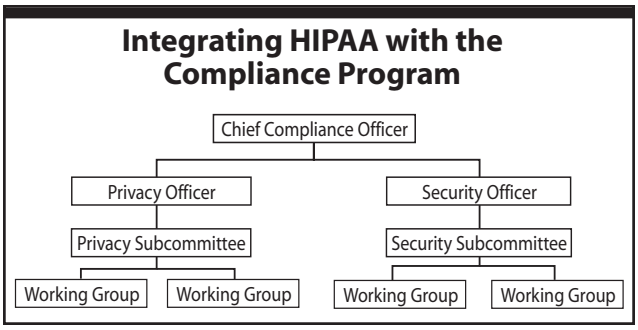
Among recent fraud settlements or investigations involving false claims or billing:

❖ Catholic Healthcare West and Mercy Healthcare Sacramento, the largest Catholic hospital system in the West, have agreed to pay the Federal Government $10.25 million to settle a whistleblower's allegations that its Sacramento facility lied on Medicare and Medi-Cal claims. The government alleged that from 1992 to 1999 the hospital system submitted claims for non-reimbursable annual physical exams, claims that depict routine physician referrals as more expensive consultations, and claims for undocumented lab work and other ancillary services. Under terms of the deal, the hospital system admitted no wrongdoing. Whistleblower George Baca, former head of patient business services at a facility in the CHW system, will receive more than $1.85 million as his share of the recovery.

❖ Seven hospitals in Arizona, California, and Florida have agreed to pay $5.5 million to settle charges that they unlawfully billed federal healthcare programs for surgical procedures using experimental cardiac devices, DOJ announced in June. The procedures were performed between 1987 and 1994, using devices that had not been approved for marketing by the Food & Drug Administration. The settlement stems from a whistleblower lawsuit filed by Kevin Cosens, a former medical device salesman. He will receive nearly $1.1 million as his share of the recovery.

❖ DOJ has offered to settle an investigation into the billing practices of Unilab Corp. (Tarzana, CA) for $2.8 million, according to the lab company, one of the largest independent clinical lab testing companies in the country. Unilab, which revealed the offer in a filing with the Securities & Exchange Commission (SEC), has not yet said whether it plans to accept the offer. DOJ reportedly had been investigating Unilab's billing for four types of medical tests in the mid-1990s. Unilab previously settled investigations into its past marketing and billing practices for $7.2 million.

❖ DaVita Inc. (Torrance, CA) said in filings with the SEC that a Medicare carrier for its Minnesota laboratory is conducting a review of reimbursement claims from January 1996 though December 1999 and that DOJ has also requested information on the lab. DaVita said the review is similar to one being conducted at a lab it operates in Florida. The Medicare carrier for the Florida lab issued overpayment determinations totaling $20.6 million for a review period from January 1995 to March 1998 and has suspended claim payments to the lab since May 1998.



"To make it a mindset, you have to have a continuous, ongoing onslaught of information. Put updates in your employee newsletter or on your Website. Keep the information coming and keep it fresh."

Consent & Authorization Forms

Under HIPAA requirements, healthcare organizations need to pay particular attention to development of consent and authorization forms, according to King. Consent forms should be written in general terms, specifying that the entity be allowed to use or disclose patient health information only for treatment, payment, or healthcare operations. The forms should state that the provider might refuse to treat individuals who don't sign the consent form and should note that all consents may be revoked in writing.

Consent forms may be combined with other forms of legal permission if they are visually and organizationally separate, and separately signed and dated, notes King. They may not be combined with the entity's notice of privacy practices. Providers that participate in an organized healthcare arrangement with another healthcare provider can use a joint consent form, she adds, if they provide a joint notice of privacy practices.

HIPAA regulations do specify certain exceptions to obtaining consent, such as cases where the provider has an indirect relationship with the patient, where the patient is an inmate, or in emergency situations. In these cases, documentation is critical, says King. The provider needs to show valid reason why consent could not be obtained.

While consent forms are fairly general and are used for treatment, payment, and operations issues, authorization forms are more specific and allow use and disclosure for purposes other than what is covered by the consent.

"Authorizations are written in specific terms," notes King. "They specify who is going to get what information and why; there's a time limit on it. Treatment cannot be conditioned on signing, whereas on consents it can be. Authorizations can be revoked at any time in writing."

King suggests that providers conduct an inventory of current consent and authorization forms. Determine what you have, who's using them, and whether you keep copies in medical records. Once you have a good understanding of how consents are handled currently, it's time to make decisions about how they will be handled under the privacy regulations.

"Are you going to do them at the front door, are you going to do them on the floor, who's going to be responsible, and who's going to monitor them?" she asks. "These are all things you have to decide."

Due Diligence

Ultimately, intent will play a key role in determining whether you have satisfied HIPAA requirements in instances where the facility may have to defend itself, notes King.

"You need to be able to show that you are going about this with a clean heart and that you're trying to comply. That will go a lot further if you have a problem than saying, 'Gosh, we didn't know and it seemed hopeless, so we didn't try.'"

King suggests that providers keep a diary of efforts taken to begin developing HIPAA compliance policies. Document seminars that staff have attended, meetings held, projects begun. "You want to be able to show where you started, and even if you haven't gotten where you're going by the compliance deadline, you can show that you've made a good-faith effort."

Resource

❖ Carrie King: 713-794-4000

Rehnquist Nomination As IG: *Could It Spell Changes Ahead?*

If confirmed by the Senate, the nomination of Janet Rehnquist as Inspector General of the Department of Health & Human Services could potentially change the way that corporate integrity agreements and voluntary disclosures are handled, according to healthcare sources.

Rehnquist, an assistant U.S. attorney for the Eastern District of Virginia, was associate counsel to former President Bush from 1990 to 1993 and has worked as counsel to the Senate's permanent subcommittee on investigations. She is the daughter of U.S. Supreme Court Justice William Rehnquist.

Because of her background and links to the Bush Administration, Rehnquist may be more likely to take the side of the Department of Justice in areas where Justice and the HHS Office of Inspector General have disagreed, including the OIG's use of corporate integrity agreements (CIAs), sources speculate. In general, Justice has not supported widespread use of CIAs, fearing they might undermine the law enforcement authority of its prosecutors.

If Rehnquist were to modify the way CIAs are used, it's possible that providers operating under existing CIAs might push to renegotiate all or part of their settlement agreements, the speculation goes.

Justice and the HHS OIG have also disagreed on voluntary disclosure of compliance problems, which could have an impact on how self-disclosure is viewed under Rehnquist. The OIG favors self-disclosure, while Justice does not.

As of late June, no Senate hearing on Rehnquist's nomination had been scheduled.

OIG/GAO Warning, *from page 1*

raise concerns for providers. While some of the practices themselves may not rise to the level of fraud and may not be illegal in all cases, they do increase the risk of abuse of the Medicare and Medicaid programs, according to the bulletin.

"We encourage providers to recognize and protect themselves and the programs against these questionable practices," the OIG advises. The oversight agency does, however, acknowledge that responsible consultants play an integral role in developing and maintaining practices that enhance a client's business objectives as well as in improving the overall integrity of the healthcare system.

"We believe that most consultants, like most providers, are honest and that the vast majority of relationships between providers and consultants are legitimate business activities," says the OIG.

"Unfortunately, a small minority of unscrupulous consultants engage in improper practices or encourage abuse of the Medicare and Medicaid programs. Depending on the circumstances, these practices may expose both the consultants and their clients to potential legal liability. Hiring a consultant does not relieve a provider of responsibility for ensuring the integrity of its dealings with federal healthcare programs."

Questionable Practices

To safeguard themselves, the OIG advises, providers engaging the services of consultants should be alert to the following questionable practices:

❖ **Illegal or misleading representations.** Consultants may make illegal or misleading statements or representations about their relationship with the Medicare program, the Centers for Medicare & Medicaid Services (CMS, formerly the Health Care Financing Administration) or the OIG. For example, consultants may misrepresent that they have inside or special access to the OIG or to OIG materials. In other cases, consultants may misrepresent that their services or products are approved, certified, or recommended by Medicare, CMS, the Department of Health & Human Services, or the OIG.

❖ **Promises and guarantees.** Consultants may explicitly or implicitly promise or guarantee specific results that are unreasonable or improbable. In some cases, consultants may resort to improper means to effectuate these promises or guarantees, such as submitting false claims or preparing false cost reports on behalf of a client. This misconduct potentially subjects both the consultant and the provider to liability under the False Claims Act, says the OIG. Problematic promises would include, for example:

—A valuation consultant promising or assuring a client that its appraisal of a physician's practice will yield a fair market value that satisfies the client's need for a particular valuation, regardless of the actual value of the practice.

—A billing consultant promising a prospective client that its advice or services will produce a specific dollar or percentage increase in the client's Medicare reimbursement. The consultant's fee is often based on a percentage of this increased reimbursement, notes the OIG.

❖ **Encouraging abusive practices**. Some consultants may knowingly encourage abuse of the Medicare or Medicaid programs, says the OIG. In some cases, reimbursement specialists or other consultants advocate that their clients engage in aggressive billing schemes or unreasonable practices that are fraudulent, such as suggesting that a client use inappropriate billing codes in order to elevate reimbursement, describing methods to avoid detection, or advising a client to bill for an expensive item or service when a less expensive item or service was actually provided.

❖ **Discouraging compliance efforts**. Some consultants may make absolute or blanket statements that a client should not undertake certain compliance efforts (such as retrospective billing reviews) or cooperate with payer audits, regardless of the client's circumstances. As reflected in the OIG's compliance guidance, the OIG believes that voluntary compliance efforts, such as internal auditing and self-review, are important tools for doing business with federal healthcare programs. Left undetected and, therefore, unchecked and uncorrected, improper billing or other conduct may exacerbate fraud and abuse problems for a provider in the future.

Resources

❖ GAO report, "Health Care: Consultants' Billing Advice May Lead to Improperly Paid Insurance Claims" (GAO-01-818), June 2001: Available online at *www.gao.gov.daybook/010627.htm*.

❖ OIG Special Advisory Bulletin, "Practices of Business Consultants," June 2001: Available online at *www.os.dhhs.gov/progorg/oig/frdalrt/consultants.htm*.

New Draft SUD Guidance

The Food & Drug Administration is seeking comments on draft premarket guidance for reprocessing and reuse of single-use devices (SUDs) in patient care. The draft supplements a final guidance published Aug. 14, 2000, "Enforcement Priorities for Single-Use Devices Reprocessed by Third Parties and Hospitals." Comments on the draft are due by this Aug. 30. The draft guidance is found online at the Website for FDA's Center for Devices & Radiological Health, www.fda.gov/cdrh. For more information, contact Tim Ulatowski, 301-443-8879.

COMPLIANCE PERSPECTIVES

Successfully Negotiating Corporate Integrity Agreements: *Responding Effectively To New Realities*

Stuart M. Gerson, Esq., is a partner with Epstein Becker & Green, PC, Washington, DC

Many commentators believed that the antagonism towards litigation and over-reaching by government that was expressed by presidential candidate George W. Bush would manifest itself in his Administration by a less-intense level of enforcement regarding healthcare matters.

Such wishful thinking, however, has been exploded by converging factors, including the emerging national consensus on a patients' rights bill with litigation remedies; the re-promulgation of broad, enforceable privacy regulations; and aggressive statements about enforcement by newly-installed governmental officials.

These factors gave additional weight to the U.S. Supreme Court's categorical rejection of the constitutional arguments against the *qui tam* (whistleblower) provisions of the federal False Claims Act (FCA).

Given this new reality, healthcare providers are compelled to recognize the likelihood that, at some point, they will be the subjects of investigations, and to be aware of the panoply of legal tools that could be arrayed against them.

In the government's ongoing and expansive campaign against healthcare fraud, the Corporate Integrity Agreement, or CIA, has become the tail that wags the False Claims Act dog.

Immediately following the 1985 amendments to the FCA, a civil-case defendant essentially had only the Justice Department (DOJ) to worry about.

This was, and is, a considerable worry, given the FCA's treble damages and additional monetary penalties per unlawful claim, the fact that the government's civil burden of proof is not a stringent one (specific intent to defraud is not an element), and the vast proliferation of FCA cases—in many instances brought in the name of the United States by *qui tam* relators. These factors made civil settlements far more numerous than fully litigated cases.

However, as the government's enforcement regime matured, the Department of Health & Human Services' Office of Inspector General (OIG), with its Damoclean power of exclusion, became at least as formidable as DOJ.

While the settlement trend continued, the settlement paradigm itself shifted. The basic dollar outlays remained the purview of DOJ, and in most cases, the OIG has elected to waive civil and administrative penalties, but only in consideration of the settling defendant's adoption of a fully functional CIA. These agreements are often more complex than the settlement agreements negotiated by DOJ and, increasingly, their costs rival those paid through DOJ.

Recent Benchmarks

In just the past six months alone, the OIG has entered into CIAs with a range of providers, both large and small, including The Healthcare Company (the former Columbia/HCA), LifePoint Hospitals Inc., Rehabilicare Inc., Bayer Corporation, The Center for Health and Human Services Inc., Carrollton Emergency Physicians PC, West Virginia University Medical Corporation d/b/a University Health Associates, Arlington Emergency Medicine Associates, Emergency Medicine Specialists of Orange County, Kern Emergency Physicians, and Paracelsus Healthcare Corporation.

The range includes providers in virtually all aspects of healthcare—from hospitals to pharmaceuticals and other manufacturers to physician groups. This form of unwelcome diversity shows the breadth of the government's anti-fraud efforts that often are aided by *qui tam* relators.

In each of these cases, the OIG waived exclusion of key provider entities and substantially waived civil and administrative penalties beyond the monies paid through the CIA.

Even where a criminal conviction mandated exclusion, the government confined the remedy to limited areas of the business, leaving

important numbers of providers still operative.

The cost of this waiver is high, and providers anticipating a CIA should focus on the conditions imposed to determine where and how their negotiating skills should be directed.

A five-year term has become the norm, though some are now imposed for as much as eight years. The former three-year mean term has become increasingly rarer.

Each recent CIA set forth specific review guidelines and required retention of an Independent Review Organization (IRO). Each entity was required to provide the OIG with a written report demonstrating its compliance with the CIA and to submit annual written reports thereafter.

In some instances, the CIA included detailed work plans that described the specific review procedures that the entity and the IRO must follow. The OIG always reserved its right of inspection, audit, and review.

The integrity obligations imposed and enumerated in the CIAs generally included requirements regarding compliance officers and committees, written policies and procedures, training and certification, third-party billing, annual review procedures, reporting of overpayments and material deficiencies, and notification of government investigations or legal proceedings.

The CIAs also included requirements imposed on the entity regarding notification and submission of reports, retention of documents and records, disclosures, and included a breach and default provision. In some instances, the CIA also included a provision requiring the entity to notify the OIG within 30 days of a change of its ownership, location, or purchase or establishment of a relevant new business.

Given This Burden, Can You Avoid A CIA?

The answer is probably not, but there are a number of useful things that any provider can and should do in advance of having an actionable problem (and, hopefully, to avoid one altogether), at least to minimize the scope and cost of any CIA that might be imposed if there is future difficulty.

First, recognize that the OIG's regimes are outcome-driven and in approaching the agency initially, be prepared to make a detailed presentation as to the corrective action already taken. If the problem is small and the correction is demonstrably effective, your bargaining position will be substantially improved.

Second, be aware that a CIA is, essentially, a variant of the OIG's compliance guidance, but with greater focus as to the problem at issue and with a substantial audit and reporting function. Having such a program in place can minimize ancillary CIA requirements if the key elements of the OIG's compliance guidelines are in place. These include:

- ❖ Written standards of conduct for employees.
- ❖ Distribution of written policies that prospectively address specific areas of potential fraud, such as billing, marketing, and claims processing.
- ❖ Designation of a chief compliance officer charged with operating the compliance program.
- ❖ Providing educational and training programs to all employees.
- ❖ Audits and/or other evaluation techniques to monitor compliance and ensure a reduction in identified problem areas.
- ❖ Use of disciplinary action against employees engaged in wrongdoing.
- ❖ Investigation and remediation of identified systemic and personnel problems.
- ❖ Using adherence to compliance as an element in evaluating supervisors and managers.
- ❖ Development of policies addressing the termination or retention of sanctioned individuals.
- ❖ A hotline to receive complaints, while protecting the anonymity of complainants.
- ❖ Record creation and retention policies.

What Criteria Should A Provider Be Prepared To Address In Negotiations?

Basic Criterion

The CIA is tailored to the specific provider and relates to the facts and elements of the underlying case (FCA, kickbacks, racketeering, etc.). The provider should negotiate to limit this scope as much as possible.

Duration

While three-year agreements once were prevalent, the typical CIA today is for a period of five years and even has reached eight. The better the compliance program already in place, the more likely a maximum term can be avoided.

A good negotiator should consider the possibility of easing outside review and other commitments based on demonstrated good behavior during the CIA period. This is significantly more probable than shortening the term itself.

Commitments

Similar to the OIG's compliance guidance, the settling provider must be prepared to guarantee the following:

- ❖ Hiring or maintaining a compliance officer and having a compliance committee.
- ❖ Developing written policies and standards.
- ❖ Implementing a comprehensive employee training program.

- ❖ Establishing an auditing regime for federal billings.
- ❖ Restricting employment of excluded persons.
- ❖ Providing for independent verification of data submitted.
- ❖ Submitting periodic reports and consulting with the OIG.

These commitments are unavoidable. However, again by demonstrating the utility of the functions already in place, the negotiator might limit the scope and expense of the "add-on," particularly the IRO.

Relevant Concerns

The OIG will require the CIA negotiator to address a number of substantive issues, including:

- ❖ The nature of the conduct that led to the action.
- ❖ The culpability of the provider (rogue employee, newly-acquired venture, etc.).
- ❖ Whether the event is the first or a repeat.
- ❖ The nature of the corrective action undertaken (and if any such action was taken, *e.g.*, through a voluntary disclosure, before government involvement).
- ❖ Whether the problem was isolated or system-wide.

The Ultimate Goal

In addressing these concerns the ultimate goal is, as much as possible, to try to convince the OIG that the CIA might be adapted to a voluntary compliance program already in place.

The main issue of burden and expense, as noted, is whether a provider's internal auditing component may conduct all initial review, subject to OIG oversight, or whether an IRO must be retained.

Likely Responsibilities

Outside review is the greatest CIA burden, but not the only one the negotiator must be prepared to address. Probable responsibilities under a CIA include:

Notice: The CIA Covered Entity must issue notice that includes informing the Covered Persons of the existence of the CIA and the nature and scope of the obligations imposed.

General Compliance Training: The Entity must provide general training to all Covered Persons on the CIA, the compliance program, and the code of conduct. Generally, within 60 days of the CIA's effective date, all Covered Persons not already trained must be trained.

Functional Compliance Training: In addition to general training, all Covered Persons usually must receive at least two hours of compliance training relating to legal and regulatory issues specifically affecting their business segment. The deadline for this training depends on the size of the organization, but it can be negotiated to extend over a period of months following the CIA's effective date.

Specialized Training: As to particular subject content, specialized training must be provided within a negotiated period.

Sales & Marketing Personnel: Where applicable, all persons responsible for sales & marketing activities must receive training relating to legal and regulatory issues affecting these responsibilities. This is particularly applicable to a case based on a kickback theory. So, in order to limit this criterion, the negotiator should attempt to minimize the issue by stressing compliance in place and adherence to safe harbors, etc.

Specialized Training For Billing Personnel: This one is unavoidable, so save your negotiating energies for something else. Generally, all persons who participate in the preparation or submission of bills, claims, and/or cost reports must, within stated periods, receive at least six additional hours of training relating to legal and regulatory issues affecting these responsibilities.

Medical Director Training: All physicians who serve as medical directors usually must receive at least two hours of baseline training and education and annual supplemental compliance training as soon as is practicable following the execution of the CIA.

Supplemental Training: Pursuant to a comprehensive plan that the Covered Entity must submit, it must include a period of supplemental compliance training on an annual basis. The amount of such training and the employees covered are negotiable.

Organizational Scope Of Responsibility: If the Entity has or forms an affiliate, it needs to ensure that such affiliate agrees to satisfy the requirements of the CIA.

Similarly, the Entity shall require that its contractors acknowledge the CIA and the Entity's compliance program and code of conduct.

The OIG is rarely impressed with arguments that this requirement adds to the Entity's costs and thus favors its competitors.

Indeed, the OIG is not undesirous of leveraging individual CIA

CIAs On The Web

The HHS Office of Inspector General's Website has a current listing of corporate integrity agreements, frequently asked questions about CIAs and major provisions, and a content checklist for the annual reporting required under a CIA. Go to the OIG's home page at www.hhs.progorg.oig

requirements into model compliance industry standards.

IRO Responsibilities: As noted repeatedly, unless the settling Entity can convince the OIG that its internal audit and compliance functions are sufficient to provide appropriate oversight, the Entity will be required to retain an IRO to assist in assessing the effectiveness of its policies and procedures as well as the compliance practices mandated by the CIA.

Your best ultimate protection against the added burdens of a corporate integrity agreement is to have a strong compliance program that can be adapted, if necessary, to CIA requirements. Your second best line of defense is intelligent negotiation of the CIA, with a main focus on limiting outside review

Avoidance of the IRO function is very unlikely in any case that involves billings. If the FCA action is predicated on something else—for example, a minor erroneous certification of eligibility for reimbursement—avoidance of the IRO is a possibility.

A more practical goal is a reduction in the out-years of IRO functions, *e.g.*, number of cases reviewed, based on demonstrated good compliance in the initial years of the CIA.

In the likely event that there will be an IRO requirement, it will include, depending on the nature of the settling entity, a work plan occasioning annual analysis of a host of issues, including cost reports, billing procedures and verification, credit balances, contracts, laboratory services, clinical diagnostic services, etc.

Statistical Sampling: Whether or not accomplished by an IRO, all statistical samplings or appraisals must use the OIG's Office of Audit Services Statistical Sampling Software, also known as RAT-STATS.

Screening Requirements: A CIA-covered party may not employ or engage as contractors any person who is excluded (or suspended or debarred) from a federal healthcare program or has been convicted of a criminal offense related to the provision of healthcare, and must periodically compare its list of employees and contractors against the exclusion list.

Reporting Requirements: Any Entity covered by a CIA will have certain periodic reporting requirements to the OIG, including:

- Prompt notification of any ongoing investigation or legal proceeding by a governmental entity involving an allegation of fraud.
- Notification to payers, generally within 30 days of discovering an overpayment, with remedial steps to follow within 60 days to correct any operational or policy deficiencies.

CIAs also often require parties to report to the OIG concerning:

- Substantial overpayments.
- Potential violations of criminal, civil, or administrative law.
- Violations of obligations to provide items or services under professional recognized standards.
- New locations or business units.

More generally, CIAs require an initial written report, usually after six months, on the status of implementation of the CIA's requirements and annual overall compliance reports thereafter for the duration of the Agreement.

If You Make the Agreement, You Must Keep It: Failure to comply with the requirements of the CIA can result in monetary penalties and/or exclusion from federal healthcare programs. Such failures also can implicate the settlement agreements reached with the Justice Department.

Conclusion

An analysis of operative realities sometimes offers little cause for optimism. The foregoing discussion fits that bill.

The government's anti-fraud activities are consistently on the increase, as are related *qui tam* actions. Given the lenient burden of proof (no specific intent required), the equivocal nature of much that relates to healthcare reimbursement, and the onus of potential exclusion, the vast majority of defendants will settle with the government, and that, almost always, will mean a CIA.

The best ultimate offense, therefore, is a pre-existing defense, *i.e.*, a strong compliance program that can be adapted to CIA requirements. The second best offense is intelligent negotiation of the CIA itself, with a prime focus on limiting outside review.

Significantly, the government has almost uniformly demanded, as a condition of settling fraud investigations in the burgeoning healthcare area, that the defendant abide by a Corporate Integrity Agreement, which can be burdensome and entail substantial government oversight and outside expert involvement, elements that are not necessarily part of a voluntarily adopted corporate compliance program.

❖ *Mr. Gerson may be contacted at Epstein Becker & Green, Ste. 700, 1227 25th St. NW, Washington DC 20027. Tel: 202-861-0900. E-mail: sgerson@ebglaw. com*

Former Lab Exec Pleads Guilty In ESRD Case
Double Billing Fraud Charges Dropped

The former president of LifeChem Inc., Eileen Aird, has pled guilty to knowing about but failing to report the company's double billing to Medicare for certain tests performed on patients with end-stage renal disease (ESRD) in the early 1990s.

The guilty plea was part of a settlement in which the government agreed to drop charges that Aird had conspired to defraud Medicare by tricking doctors into ordering medically unnecessary hepatitis C tests, then billing Medicare for the tests performed by LifeChem, according to one of Aird's attorneys, Marty Rogers.

Aird will be sentenced Sept. 13, 2001, and faces a statutory maximum of up to three years in prison and a $250,000 fine, although Rogers, with the Washington, DC office of Ober/Kaler, says she hopes and expects Aird to receive probation and only a small fine, if she receives one at all.

Concealment Alleged

In pleadings filed in U.S. District Court on June 11, the government charged Aird with concealing and failing to report a crime by LifeChem from July 1992 through August 1995. Federal attorneys alleged that Aird concealed the submission to Medicare of duplicate claims for payment for laboratory blood tests performed between February 1991 and June 1992.

The claims, the government says, were accompanied by the false representation that the tests were lawfully payable as non-routine blood tests when, to the contrary, Medicare had already paid for the tests as routine blood tests for dialysis patients. According to the charges, this resulted in the lab's double billing of the Medicare program for approximately $4.9 million, an amount subsequently repaid as part of a voluntary disclosure in the fall of 1995.

Faulty Computer Systems

The double billing, agree the government and Aird, actually resulted from inaccurate claims generated by a new computer billing system installed by LifeChem in 1990. In June 1992, LifeChem fixed the system so that it stopped the double billing.

However, the government alleges that between July 1992 and August 1995, LifeChem failed to report the double billing to the Medicare carrier or the Health Care Financing Administration and did not promptly refund the money owed.

> *The double billing, agree the government and Aird, resulted from inaccurate claims generated by a new computer billing system. The government alleges that LifeChem failed to report the double billing and return the money*

Aird maintains that she is innocent of the charge that she conspired to defraud Medicare by tricking doctors into ordering medically unnecessary hepatitis C tests, but she agreed to a plea of failing to report LifeChem's double billing. Aird accepted the settlement because of health reasons, says Rogers.

In exchange for Aird's guilty plea, the government has dropped charges brought in 1999 that Aird and the former product manager for LifeChem conspired to defraud Medicare by performing and billing for medically unnecessary tests.

Case To Be Dismissed

"The government tried to hold Eileen criminally responsible for the medical necessity of tests ordered by doctors, but if the doctor orders them, the lab is supposed to perform them," says Rogers. "That case will be dismissed when Eileen is sentenced on Sept. 13."

Between 1990 and 1996, Aird was general manager and president of LifeChem (Rockleigh, NJ), a subsidiary of National Medical Care Inc. (Waltham, MA). NMC was the largest provider of services to patients with ESRD in the U.S. In October 1996, it was purchased, along with its subsidiaries (including LifeChem), by Fresenius Medical Care, based in Lexington, MA.

In September 1999, the government charged Aird and Louise Verde, former LifeChem product manager, with devising and executing a scheme from the early to mid-1990s to induce the ordering of medically unnecessary tests for ESRD beneficiaries.

The case against Verde was dismissed by the government late last year, says Rogers. Margaret Telgheder, a former vice president of the Medical Products Division of NMC, pled guilty to the offense in June 1999.

Other Executives Charged

Also in 1999, the government separately charged two other NMC executives with providing kickbacks to obtain ESRD testing business for LifeChem. David Weber pled guilty to that offense in December 1998.

Glenn Shaw, former president of NMC's Medical Products Division, is scheduled to go to trial in September, according to Rogers.

Compliance Tips For Developing A Direct Access Testing Program

As one of the fastest growing trends in the laboratory industry, direct access testing (DAT) potentially can help labs grow their business if they are careful to address compliance and liability concerns before offering the service, say two operators of labs that offer it.

Under DAT, the consumer pays out-of-pocket to order certain tests from a testing facility and receive the test results. State law governs the matter. There is no federal law either for or against it.

While many states don't allow any kind of direct access testing or limit the tests that may be provided, DAT has the potential to become a significant segment of the lab market in the states that do allow it, believes R. David Carrozza, owner and operator of The Lab (Folsom, CA). DAT constitutes about 10% of The Lab's business.

"I think this has the potential to be the hottest growth curve for the lab industry in the next 10 years," he says. "Baby boomers have high service expectations and high disposable income, and the Internet offers something like 600,000 different Websites that relate some way to healthcare."

California currently allows labs to provide four self-authorized tests—pregnancy, glucose, fecal occult blood, and cholesterol—although the state legislature is considering legislation that would allow an expansion of the DAT menu. Some states, such as Texas, Ohio, and South Dakota, have no limits on direct access testing, while others, including Florida, Illinois, and Pennsylvania, do not allow it at all, according to the American Society of Clinical Pathologists.

While not necessarily a big money-maker, DAT is useful in helping labs become better known in the community, which can lead to growth in the business as a whole, explains Carrozza.

"It's profitable, but its potential has more to do with building a clientele and providing a community service. The key is making it affordable and convenient for people."

Bill Hofer, director of business development for Clinical Laboratories of the Midwest (CLM—Sioux Falls, SD) also sees DAT as a growing sector of the lab industry. CLM, which has two patient service centers, currently offers 15 tests that can be ordered by an individual without receiving physician authorization (*see sample menu*).

"We're seeing more and more people come in to order tests on themselves," notes Hofer. "The common lay person is getting pretty sophisticated these days in understanding laboratory tests, and since Medicare does not pay for screening tests, we're seeing Medicare patients coming in more."

While DAT constitutes less than 1% of CLM's business, Hofer expects that number to increase. "We've deliberately kept it small. We wanted to just get our foot into it and establish the systems and processes, knowing that in the future this product line is going to grow."

For labs interested in developing a DAT program, Hofer and Carrozza offer the following tips:

❖ **Determine which tests to offer**. In states where the DAT menu is limited, this is an easy decision, but in states that don't restrict DAT, the lab operator must decide whether or not to offer tests that can require exten-

Sample Direct Access Testing Menu

While the range of direct access tests allowed varies by state, the following is a sample of tests that individuals can request from Clinical Laboratories of the Midwest in Sioux Falls, SD.

Test Name & Components	Fee	Results Available
ABO/Rh blood type	$25	Following day after 2 p.m.
CBC (WBC, RBC, hemoglobin, hematocrit & differential)	$20	Following day after 9 a.m.
Cholesterol	$15	Following day after 9 a.m.
Comprehensive metabolic panel	$23	Following day after 9 a.m.
Drugs of abuse (amphetamines, cocaine, opiates, marijuana, PCP)	$45	24-48 hours
Glucose	$15	Following day after 9 a.m.
Hemoglobin A1c (glycated hemoglobin)	$30	Following day after 9 a.m.
Lipid panel	$39	Following day after 9 a.m.
Mononucleosis screen	$18	Same day within 2 hours
Pregnancy	$24	Same day within 2 hours
Prothrombin time	$24	Same day within 2 hours
Prostate-specific antigen	$40	Following day after 9 a.m.
Strep screen	$25	Same day within 2 hours
Thyroid stimulating hormone	$45	Following day after 9 a.m.
Urinalysis	$24	Same day within 2 hours

Source: Clinical Laboratories of the Midwest. Reprinted with permission.

sive follow-up, such as HIV testing. Neither CLM nor The Lab offers HIV testing on a direct access basis. "We made a conscious decision not to get into that realm, although for some labs that do direct access testing, that's their number one test," says Hofer.

❖ **Check applicable laws and certification requirements**. Find out what the law is in your state regarding DAT, says Hofer. Also find out if your accrediting body has any restrictions on it. The College of American Pathologists, for example, says tests must be ordered by "a physician or other authorized person." This requirement, again, refers you back to state law to determine if individuals may self-order tests, notes Hofer.

❖ **Make sure individuals understand their responsibilities**. CLM has all individuals who order direct access tests sign a waiver, indicating that they understand the limitations of test results and acknowledging that they are responsible for any follow-up with their physician. This helps reduce any potential lab liability, Hofer says.

❖ **Establish a review system**. Because DAT results are sent only to the individual, not the person's physician, it's important to establish what to do in case of significantly abnormal results, say both Hofer and Carrozza. "We've had a couple of cases where people had critical values on glucose," explains Carrozza. "In those cases, we contacted the patients immediately and recommended that they get right in to see a doctor."

❖ **Be sensitive to confidentiality and privacy issues**. Although new patient privacy requirements mandated by the Health Insurance Portability & Accountability Act (HIPAA) won't take effect until April 2003, you should already be incorporating those protections into your processes. For example, if you are considering allowing individuals to access their results over the Internet, you will need to ensure that the information cannot be accessed by anyone but the person ordering the test. "HIPAA steps privacy concerns up a notch," notes Hofer.

Be careful about calling individuals with test results, adds Carrozza. The Lab never phones clients; instead, people who order tests are given a number and must call The Lab to receive test results. "Privacy is an important issue for us," he says. Clients can then choose to receive their results through the mail.

Resources

❖ David Carrozza: 916-983-3522
❖ Bill Hofer: 605-328-5458

So Long HCFA, Hello CMS: Officials Promise "More Responsiveness"

Health & Human Services Secretary Tommy Thompson announced recently that the current Health Care Financing Administration is being restructured and has been renamed to better reflect the mission of the agency and allow it to be more responsive to beneficiaries and providers.

As part of the restructuring, HCFA has been christened the Centers for Medicare & Medicaid Services (CMS), which will be organized around three main centers that reflect the agency's major lines of business:

❖ The Center for Medicare Management will focus on traditional fee-for-service Medicare, including development of payment policy and management of fee-for-service contractors.
❖ The Center for Beneficiary Choices will focus on providing beneficiaries with information on Medicare, Medicare Select, Medicare+ Choice, and Medigap options. It also will handle management of Medicare+Choice plans, consumer research and demonstrations, and grievance and appeals functions.
❖ The Center for Medicaid & State Operations will focus on programs administered by the states. This includes Medicaid, the State Children's Health Insurance Program, insurance regulation functions, survey and certification, and lab oversight under CLIA (Clinical Laboratory Improvement Amendments).

According to the new CMS head, Thomas Scully, the restructuring of the agency should make it easier for providers to understand the various programs or get answers if they do not. Also, fewer internal meetings will be scheduled, he said, to free up officials to work with providers.

During recent testimony before a congressional committee, Thompson said one of his top priorities will be to improve CMS's responsiveness by eliminating regulatory red tape; establishing key contacts for beneficiary groups, health plans, physicians, providers, and suppliers; and enhancing outreach and education.

As part of these changes, Thompson is forming a new Departmental Task Force on Regulatory Reform, which he says will focus on eliminating unnecessary burdens and duplicative paperwork caused by federal regulations that are hurting patient care.

American Hospital Association president Dick Davidson applauded the focus on regulatory reform. "Secretary Thompson has thrown a lifeline to the nurses, doctors, and others across this country who are drowning in a sea of paperwork. This holds out hope that caregivers can get back to what really counts: caring for patients."

The Back Page

News-At-A-Glance

Fraud Settlement: HealthSouth Corporation (Birmingham, AL)—the Nation's largest provider of outpatient surgery, diagnostic imaging, and rehabilitative services—has agreed to pay $7.9 million to settle healthcare fraud allegations, according to the Department of Justice. The government alleged that the company had overcharged Medicare and the Defense Department's TRICARE program for equipment and supplies purchased from G.G. Enterprises, a corporation owned by the parents of HealthSouth's CEO, Richard Scrushy. The government said HealthSouth improperly billed these items at a price above G.G. Enterprise's costs, in violation of Medicare's and TRICARE's rules for transactions with related entities.

Lab Company Settles: Urocor Inc. (Oklahoma City, OK), which specializes in tests to detect bladder and prostate cancer, has agreed to pay $9 million to settle allegations that it overcharged federal healthcare programs for tests it performed, according to the Department of Justice.

The settlement stems from allegations made by four whistleblowers who asserted the company billed Medicare, TRICARE, and other federal healthcare programs for medically unnecessary and investigational tests.

The company also has entered into a five-year corporate integrity agreement (CIA) with the HHS Office of Inspector General, says Justice. The CIA requires the company to maintain its current compliance program in addition to fulfilling "certain integrity obligations" not in place before.

Safety Needle Citation: Cal-OSHA has cited a Kaiser Permanente hospital in Los Angeles for failing to ensure that devices with engineered sharps injury protection were used as required and for failing to ensure that contaminated sharps were not removed from devices. The hospital faces possible penalties of $19,120 for these citations and another $1,275 for allegedly failing to fill out its sharps injury log completely and for alleged inadequacies in its bloodborne pathogen exposure control plan.

The citations were made under California's bloodborne pathogen standard and resulted from an inspection that began Nov. 21, 2000, according to Cal-OSHA. Kaiser Permanente plans to contest the citations and expects them to be ultimately dismissed, says a spokesman.

Improper Transfers: Christus Schumpert, a hospital in Shreveport, LA, will pay the government $125,000 to resolve claims arising under the False Claims Act after the Justice Department alleged that the hospital improperly billed Medicare for patients who were transferred to other hospitals. Under Medicare prospective payment (PPS), hospitals receive a per diem rate for patients they transfer to another PPS hospital, rather than a fixed rate.

Justice charged that Schumpert intentionally submitted false Medicare claims for full payments for patients who were transferred from Schumpert to other PPS hospitals, rather than discharged. As part of the settlement, the government extensively reviewed the hospital's compliance program and decided not to institute a Corporate Integrity Agreement.

G-2 Compliance Report (ISSN 1524-0304). © 2001 Washington G-2 Reports, 1111 14th St, NW, Suite 500, Washington DC 20005-5663.
Tel: (202) 789-1034. Fax: (202) 289-4062. Order Line: (212) 629-3679. Website: www.washg2.com.