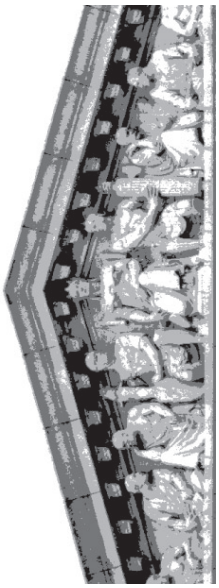


G-2 Compliance Report

WASHINGTON G-2 REPORTS

Vol. VI, No. 10, Nov-Dec 2004

For Hospitals, Laboratories and Physician Practices

OIG Sets Focus Areas For 2005
Pathology Arrangements Among Targets

Reviewing the relationships between physicians who furnish pathology services in their offices and outside pathology companies will be among the top priorities for the Health and Human Services Office of Inspector General (OIG) in 2005, the agency says in its latest work plan.

The plan, issued each October, is a blueprint for healthcare providers on what the government intends to audit, evaluate, and investigate during the coming federal fiscal year (which runs from October 1 through September 30). Healthcare providers should use the work plan as a road map for ongoing internal compliance efforts, experts advise.

Medicare pays more than $1 billion annually to physicians for pathology services, according to the OIG. Recently, the relationships between physicians and outside pathology companies have come under increased scrutiny as a growing number of specialty physicians establish "pod" labs.

Under these arrangements, a facility manager establishes a turnkey lab for physician groups. The lab is compartmentalized in a separate building, often out of state, with separate office suites or cubicles for each of 10 or 15 physician groups. The lab provides technical personnel who work in the rooms, preparing samples for pathologists. ➥ *p. 2*

Challenges & Uncertainties Of Lab Compliance

Clinical laboratories must comply with multiple laws, regulations, and alerts, many of which are subject to some interpretation. The challenge of interpreting and meeting these mandates can be quite daunting at times, notes Carrie Valiant, an attorney with Epstein Becker & Green (Washington, DC). Valiant discussed some of the most critical compliance challenges facing labs during Washington G-2 Report's annual Lab Institute, held September 29 to October 2 in Arlington, Virginia.

OIG Fraud Alert Revisited

While the lab fraud alert issued by the Health and Human Services Office of Inspector General (HHS OIG) in October 1994 clearly limited clinical laboratories' provision of computers or fax machines to physician offices, questions still remain about what the alert did not address, believes Valiant.

The fraud alert, "Arrangements for the Provision of Clinical Lab Services," stated that the provision of computers or fax machines by a lab to physician offices could implicate the anti-kickback statute, unless the equipment is used exclusively in conducting work for the lab.

➥ *p. 9*

Inside this issue

OIG Work Plan, *from p. 1*

Generally, the lab provides the pathologist, the space, and the technical services, but the physician groups handle the Medicare billing as if they were doing the lab and pathology work themselves.

The work plan lists hundreds of studies the OIG has planned for the upcoming year, ranging from an evaluation of drug pricing mechanisms for Medicare and Medicaid to a review of whether hospitals are properly reporting rebates on Medicare cost reports. While many of the OIG's studies are ongoing, a number are new starts.

Here's a rundown of what the OIG will be scrutinizing in select areas in the coming year:

- **Laboratory services rendered during an inpatient stay.** Medicare reimbursement for lab services is based on two components—physician (or professional) and technical. According to the OIG, the technical component is unallowable under Medicare. Preliminary work indicates that $73 million of laboratory services were rendered in a hospital setting during inpatient stays nationwide in calendar year 2001. This was a considerable increase in cost over similar services in prior periods. The OIG will determine what percentage of these costs are unallowable.
- **Claims paid for clinical diagnostic laboratory services.** The Social Security Act limits Medicaid payments for clinical laboratory tests to the amounts payable for the same tests on the Medicare fee schedule. This review will assess whether Medicaid payments for certain lab and pathology tests exceeded Medicare rates for the same tests. Prior OIG work, as well as discussions with officials from the Centers for Medicare and Medicaid Services, indicated that one state continues to submit Medicaid claims that exceed the allowable rates.
- **Contractual arrangements with suppliers.** The OIG plans to evaluate contractual arrangements in which a supplier, such as a laboratory or a durable medical equipment company, agrees to operate the service on behalf of a physician's practice or hospital. Investigators will review the structure of the financial arrangements and determine whether they are having an effect on the Medicare program.
- **Compliance with select agent regulations by private and state laboratories.** The OIG will assess private and state laboratory compliance with the Department of Health and Human Services select agent regulations. Select agents are substances that could be used in bioterrorist attacks. Earlier reviews assessed compliance only at federal and university laboratories. Reviewers will assess select agent management oversight, security planning and implementation, accountability, and the identification and screening of personnel with access to select agents.
- **State public health laboratories' bioterrorism preparedness.** This review will focus on the extent to which laboratories that confirm the presence of bioterror agents are prepared to handle increased testing in a bioterrorism event or public health emergency. It will also assess the extent to which these labs are receiving support from the Centers for Disease Control to strengthen their testing capacity.
- **Smart card technology.** At CMS's request, the OIG will assess the use of "smart card" technology in Medicare demonstrations as a means of creating portable, electronic patient medical records. The review will focus on information security, data privacy, and program integrity concerns.
- **FDA oversight of blood establishments.** This study will assess the Food and Drug Administration's (FDA) oversight and review of blood establishments to ensure the safety of the nation's blood supplies. FDA is statutorily required to inspect all registered blood establishments every two years. These inspections are conducted by FDA's Office of Regulatory Affairs in conjunction with its Center for Biologics Evaluation and Research, which regulates the collection of blood and blood components and regulates related products such as blood collection containers.

Resource

OIG Fiscal Year 2005 Work Plan: *www.oig.hhs.gov/publications/workplan.html#1*

Feds Targeting Fraud By Physicians

10 Tips For Staying Off Government Radar

The federal government is stepping up enforcement actions against physicians for defrauding the Medicare program, with the number of cases more than doubling between 2001 and 2003, according to Arthur DiDio, senior counsel for the Department of Health and Human Services Office of Inspector General (HHS OIG).

The number of cases brought by the OIG against physicians involving recoveries from anti-kickback and Stark actions increased from six cases in fiscal 2001 to 15 cases in fiscal 2003, DiDio said September 27 in Baltimore. DiDio spoke at the Fraud and Compliance Forum sponsored by the American Health Lawyers Association and the Healthcare Compliance Association. The government recovered $391,000 from the six cases in 2001 and $2.19 million from the 15 cases in fiscal 2003.

Stay Off Radar Screen

So how can physicians stay off the government's fraud radar screen? D. McCarty Thornton, former HHS OIG senior counsel and now an attorney with Sonnenschein Nath & Rosenthal LLP in Washington, DC, offered 10 tips:

10 End nice personal favors to referral sources. The recent TAP Pharmaceuticals case and the OIG compliance guidance for the pharmaceutical industry effectively end an era when physicians could give gifts like NFL tickets, fancy dinners, gifts for spouses, or free computers to referral sources.

9 Don't be the low-hanging fruit. In a period of shrinking investigatory resources, don't stick out of the crowd. Healthcare fraud agents will most likely go after the most obvious fraudulent activities.

8 Be wary of being in the crowd. Don't simply follow what everyone else is doing, especially in regard to billing patterns. That's what leads to national fraud projects, such as the clinical lab audits and pharmaceutical marketing investigations of the 1990s.

7 Always start your analysis of a business arrangement with the basic purposes of the anti-kickback statute. Keep in mind that the primary purposes of the law are to prevent corruption of medical decision making, and to prevent overutilization, increased program costs, and unfair competition.

6 Get as close to a safe harbor or advisory opinion as possible. If a business deal can't fall within a safe harbor, you should document the reasons why it's not possible. Also, adopt principles from relevant OIG guidance to the extent possible.

5 Establish fair market value: "the safe unharbor." According to Thornton, the government does not want to get into a battle over what fair market value (FMV) is and is unlikely to establish an FMV safe harbor. However, there is "excellent overall protection" if FMV for a business transaction is established for necessary, justifiable services or investment by an independent, reliable source using recognized methodology.

4 Don't muddy your own shoes. In this post-Enron era, don't "fool around" with documents by shredding, altering, or backdating. Also, don't acquiesce to withholding information from the government or to producing true but incomplete information. Don't

ask for or express numeric "odds" on being detected or prosecuted.

3 Check compliance on an ongoing basis. Make sure deals are properly implemented, that parties are fulfilling substantive responsibilities, and that ongoing documentation is properly maintained.

2 Document, document, document. It is important to document the legitimate business purposes of a deal, the fair market value, the services to be provided, and the time spent providing them. Good documentation is powerful evidence of good faith and a turn-off to investigators, but documentation is a two-edged sword if it is inaccurate when created or not fulfilled going forward.

1 "Greed is good" – Not. Thornton said the "number one flag to investigators" is a return on investment that appears excessive and compensation that appears excessive. Fair market value is the key.

Physicians need to keep these 10 tips in mind as they enter into "risk areas," such as recruitment deals with hospitals, contracts for medical directorships, joint ventures, "economic credentialing" agreements, the marketing of pharmaceuticals and devices, and clinical research sponsorships, Thornton advised.

A "new, coming risk area" for physicians is in the quality-of-care area, he added. A "new enforcement paradigm" is emerging based on a pattern of unnecessary care in hospitals, together with high physician billers and administrators who don't ask questions, he warned.

Hospitals Top List Of Providers With CIAs

Hospitals account for the majority of corporate integrity agreements (CIAs) that the Health and Human Services Office of Inspector General (HHS OIG) has signed with healthcare providers in the past decade, according to an OIG official.

Since 1994, the OIG has signed a total of 941 CIAs, and 481 of them involved hospitals, said Robert DeConti, a senior counsel with the OIG. DeConti spoke September 28 at the Fraud and Compliance Forum sponsored by the American Health Lawyers Association and the Healthcare Compliance Association.

As of September 21, there were 384 active CIAs and False Claims Act settlements with integrity provisions, DeConti said, more than the number of active agreements for all of 2003 (356) and 2002 (324). However, this represents a drop from the 498 active CIAs in 2001.

Current CIAs are much more detailed that older ones, primarily at the request of providers, independent review organizations, and counsel. The evolution of CIAs also reflects the IG's experience with the documents.

Sara Kay Wheeler, an attorney with Powell, Goldstein, Frazier and Murphy (Atlanta), noted that CIAs are much more specific now than in the past, but "that does not mean that they are more onerous." In her experience, CIAs are created to be fair to providers and to target the underlying conduct that was questionable.

According to DeConti, the OIG increasingly is waiving CIAs in negotiations with providers. "This is happening more and more frequently as providers are putting in place good compliance programs," he said, noting that the OIG is sensitive to the cost of implementing CIAs and will consider less costly alternatives when appropriate.

Seattle Doctor To Pay More Than $1 Million

A Seattle doctor has agreed to pay fines, damages, and restitution totaling more than $1 million to resolve charges that she falsified claims submitted to Medicare and Medicaid between 1983 and 2004, U.S. Attorney for the Western District of Washington John McKay announced October 5.

Vimlesh Ahmad, M.D., pleaded guilty to one count of healthcare fraud for submitting claims for more expensive services than actually rendered and for services never rendered, according to McKay. Ahmad will surrender her medical license and has agreed not to practice medicine in the United States. She also will be excluded permanently from participating in federal health programs.

Investigators found that Ahmad continued the fraudulent billing practices even after making some billing changes following a 2002 audit by Washington's Medicaid agency. In one case, Ahmad billed for three visits from a patient who was out of town during the times the visits were to have taken place. In other cases, she billed for longer sessions than actually occurred.

COMPLIANCE PERSPECTIVES

The HIPAA Security Rule For Clinical Laboratories

Peter M. Kazon, Esq., is senior counsel with Alston & Bird in Washington, DC

Most laboratory providers are by now familiar with HIPAA (the Health Insurance Portability and Accountability Act) and the numerous new and highly complex requirements that it has imposed on healthcare providers. First came the HIPAA privacy rule, issued in December 2000, and subsequently simplified and revised in August 2002. Last year, the transactions and code set rule became effective, which required specific data elements to be used when billing for services electronically, as most providers were required to do, when billing Medicare. Then, in February 2003, another set of HIPAA requirements was issued, this one dealing with the requirements for electronic security. The security rule's requirements become effective for most entities on April 21, 2005, just a few short months away. The purpose of this article is to set out the basic requirements of the HIPAA security rule and to discuss how the specific requirements will apply to laboratory providers.

Covered entities must comply with the rule by April 21, 2005.

Rule Complexity

Each HIPAA regulation has brought its own special set of difficulties and challenges. The security rule presents its own complexities, partly because in many ways it is actually *less* prescriptive than other HIPAA rules. While the privacy rule and the transactions and code set rule set out specific, detailed mandates that must be followed with regard to the use and disclosure of health information and the format of covered transactions, the security rule is much more general. It sets out specific standards that must be met, but it frequently leaves it to the provider to determine what steps should be taken to achieve that standard. This is beneficial in one sense, because it gives the organization greater flexibility to establish its own security safeguards. At the same time, it also presents greater risk because, if challenged, or if a security failure occurs, the provider cannot defend itself by showing that it met the specific directives of the regulations. This may make it more difficult for an organization to show that it has done all that was reasonably required.

The security rule was published in final form on Feb. 20, 2003. The rule text establishes its basic purpose, which is to ensure the "confidentiality, integrity, and availability" of all electronic health information. "Confidentiality" means that the data is not made available or disclosed to unauthorized persons. "Integrity" means that the information has not been altered or destroyed in an unauthorized manner. And, "availability" means that data is accessible and useable upon demand by an authorized person. The security rule notes that these goals are "inextricably linked" to the goals of the privacy rule. However, the rule states that the security rule is concerned with protecting health information from unauthorized access, alteration, deletion, or transmission. The privacy rule, on the other hand, is designed to establish what information is considered "confidential" and to limit the circumstances and people designed to access, use, and disclose that information.

In addition, another important distinction between the privacy rule and the security rule is in the scope of the information that is subject to the rule. The privacy rule applies to all protected health information, even if it is not stored or used electronically. The security rule only applies to protected health information in electronic form, or "electronic protected health information," usually abbreviated as *e-PHI*. Basically, e-PHI is information that is transmitted or maintained by electronic media, which includes computers, magnetic tapes or disks, Internet, extranet, leased lines, dial up, and the physical movement of removable or transportable electronic storage me-

dia. Telephone and paper-to-paper faxes are not electronic, but telephone voice response and fax-back systems are (*i.e.*, a request for information from a computer made via voice or telephone keypad input with the requested information returned via fax). This distinction is made because the information being sent is maintained and stored on a computer.

While a great deal has been written about where to draw the line between electronic and nonelectronic information, this seems unlikely to be a large issue for most laboratories. As so much information is stored and transmitted via computer, it should be a pretty easy line for most labs to draw.

Moreover, beginning last year, most healthcare providers were required to bill Medicare electronically; thus, these providers are likely to be transmitting and storing at least that information electronically. In fact, it will probably make sense (and be easier) for organizations to apply the same basic security principles to all PHI, even that not stored electronically.

Many HIPAA resources are available online at www.nist.gov *(under publications) and at* www.wedi.org/snip

Flexible Approach

The structure of the security rule is somewhat unusual for a federal rule. It divides security requirements into three separate areas: administrative safeguards, physical safeguards, and technical safeguards. Within each of those areas, the security rule sets out a series of 18 standards that providers must take steps to implement. In most cases, the standard is followed by a series of implementation specifications, which explain how the entity is to go about meeting that standard.

To its credit, the Department of Health and Human Services (HHS) seems to have recognized that a one-size-fits-all approach would not work for security because of the variety of healthcare entities subject to the security rule. Thus, the steps that may be reasonable and appropriate for a major national laboratory to take may be different from those that would be appropriate for a hospital laboratory to take. While some implementation specifications are required, many are labeled "addressable," which means that the provider has greater discretion in determining how to comply. Standards that are labeled "required" must be implemented, but for those labeled "addressable" the provider must make an assessment of the applicability of that specification to the individual entity. If it is reasonable and appropriate, then it must be implemented. However, if the entity determines that it is not, it must document why it would not be reasonable and appropriate to do so and implement an equivalent alternative measure if reasonable.

The rule specifically envisioned a flexible approach. It specifies that in determining which security measures to use the entity can take into account the size, complexity, and capabilities of the entity; its technical infrastructure; the costs of security measures, and the probability and criticality of potential risks.

It is these last two aspects that may be most significant. First, the entity is allowed to consider the cost of different solutions in formulating its security plan; presumably, measures that may be too expensive may not be necessary. It may not make sense, for example, to build a $3,000 fence to protect a $5,000 horse, as one analyst has stated.

Similarly, the entity is allowed to determine which risks are the most probable and significant and take action against those. A laboratory may determine not to take action to protect itself from more unlikely possibilities or those that would not endanger the entire enterprise. Nonetheless, it should always be borne in mind that if there is a security failure, government enforcement agencies or private plaintiffs will look carefully at why the entity did not take particular steps.

With that background, we can examine the actual requirements that are included in the security rule. Laboratories will have to go over each of the 18 standards and the implementation specifications to determine how they will implement those requirements. If a laboratory determines that one of the implementation specifications is not appropriate and reasonable for it to carry out, it should fully document the reasons that led to that conclusion, and what alternatives it put in place, if any. The biggest threat to a laboratory would be to simply assume that the specification does not apply without analyzing its requirements and failing to document how it

reached that conclusion. If a failure subsequently occurs, it will be up to the laboratory to show why it did not follow the implementation specifications included in the rule.

Administrative Safeguards

The first set of standards relates to the administrative safeguards that should be implemented. This section includes nine basic standards and 21 implementation specifications. The administrative standards relate to the following areas:

- **Security management process**—the implementation specifications require policies related to risk analysis, risk management, sanction policy, and information system activity review.
- **Assigned security responsibility**—this requires the appointment of a security official who will be responsible for the development and implementation of the entity's policies and procedures.
- **Workforce security**—this standard will require policies related to authorization and supervision of workers; clearance procedures; and procedures to be followed when an employee is terminated.
- **Information access management**—this standard will require policies related to who has access to the facility and the data system and establish policies that document the user's right of access to health information and how it can be modified.
- **Security awareness and training**—this standard requires policies that relate to issuing periodic security reminders; protecting the system from computer viruses and other "malicious software"; monitoring who is attempting to get into the system; and procedures related to how passwords are created, changed, and terminated.
- **Security incident procedures**—this standard requires policies to identify and respond to suspected or known security incidents, mitigate the effects to extent known, and document the incidents and their outcomes.
- **Contingency plan**—this standard requires policies for responding to emergencies, such as fires, vandalism, natural disasters, or system failures, including a disaster recovery plan.
- **Evaluation**—this standard requires periodic evaluation of the security system.
- **Business associate contracts**—this standard is designed to ensure that if a business associate receives e-PHI, then the contract with the associate is amended to include specific provisions related to security.

To comply with these requirements, the laboratory will have to establish written policies and procedures to achieve the particular standards. It will then have to take the action necessary to implement those policies and procedures and to effect the necessary changes.

It may be that the risk assessment, which is required as part of the security management process, is the most important part of implementing the rule. As the rule notes, an entity must identify the risks to, and vulnerabilities of, the information in its care before it can take steps to eliminate or minimize those risks and vulnerabilities. There are a variety of approaches to performing this assessment. In performing this analysis, it will be necessary to determine where information is maintained within the laboratory and how it is used by those within the organization and where it is transmitted outside the organization. For laboratories, the information will be stored in the laboratory information systems, the billing system, and in the servers that are used to create laboratory reports. In addition, if the laboratory uses an outside billing company, it may also be maintained there.

However, it is important to remember that sensitive information may also be maintained on PDAs, laptops, various handheld instruments, and even cell phones, all of which must be considered as part of this process. This information can be accessed by billing clerks, laboratory technicians and technologists, phlebotomists, and pathologists who work in the laboratory, as well as numerous other business associates. It will be transmitted to a variety of entities, including ordering physicians, hospitals, billing companies, and often even the patient themselves.

Once the laboratory has identified where the information is maintained, who has access to it, and how it is transmitted, it can begin to identify where the system is vulnerable and where those risks are likely to come from. Common threats to healthcare information include employees; ex-employees; hackers; commercial rivals; terrorists; criminals; general public; vendors; customers; and visitors.

All of these must be dealt with in the policies and procedures established.

Physical Safeguards

The second set of requirements relates to physical safeguards. This section is fairly straightforward and establishes how to ensure that only appropriate individuals have access to facilities and the locations where e-PHI is stored. There are four standards here and eight additional implementation specifications, although some of the implementations specifications are addressable and not required. The four standards are:

- **Facility access controls**—establish procedures to determine who will have access under a disaster recovery plan; to safeguard the facility and equipment from unauthorized access, tampering, and theft; to implement visitor control and other access controls; and to document repair and modifications to doors, locks, and other similar components.
- **Workstation use**—establish procedures that ensure that the physical surroundings where workstations are set up are secure and used appropriately.
- **Workstation security**—establish standards for workstations to ensure that they are only accessible to authorized users, through both password protections and limitations on access.
- **Device and media controls**—establish procedures that govern how stored e-PHI is maintained and disposed of and how storage media, such as DVDs, CDs, and diskettes, should be handled before being reused.

For laboratories, implementing these standards will require procedures that limit who has access to various parts of the facility. Thus, no one should be allowed into the facility where confidential information is maintained without some kind of company badge or ID, and visitors should be required to check in and be closely monitored. It may also be necessary in the laboratory to react to changes in the work place, for example, when an employee is terminated to ensure that the individual is no longer able to access the premises or the system where e-PHI is maintained.

Finally, it is vitally important to monitor not only computers, but also other ancillary equipment, such as DVDs, CDs, and diskettes, where confidential information is maintained. When confidential information is deleted, it is not enough simply to hit the "delete" key on the computer because the information will continue to be available to sophisticated users. Similarly, CDs and other diskettes should not be reused until they have been fully "cleansed." If the CDs are being discarded, they must be cleansed or broken so the information is inaccessible.

Technical Safeguards

The final set of standards relates to technical safeguards, which apply to the actual software and programming that are built into the computer system to protect e-PHI. There are five standards and seven additional implementation specifications in this section. They are:

- **Access controls**—implement procedures to establish: a unique username and password for each user; technical safeguards in case of emergency; automatic log-off after a set period of time; policies related to when an individual should log off; and policies to determine whether or not to encrypt confidential information that is sent over the Internet.
- **Audit controls**—establish procedures to monitor activity on the systems, and review records to ensure the appropriateness of all activity.
- **Integrity**—ensure that no one can access e-PHI and change it inappropriately.
- **Person or entity authentication**—ensure that there are procedures in place to verify the person seeking access is the one claimed.
- **Transmission security**—ensure the integrity of e-PHI sent over the Internet or similar networks, by ensuring that it is not accessed by unauthorized individuals or changed inappropriately.

In most cases, these technical safeguards will be the guts of the laboratory's security system. For example, is information encrypted when results are sent over the Internet? How are those safeguards put in place?

All of this will require a great deal of analysis by laboratories and their business associates. Most important, it will be up to the management of the laboratory to ensure that these processes are put in place and taken seriously by all. As April will be here soon, this process should be well underway by now.

Peter Kazon, Esq., can be contacted at Alston & Bird, 601 Pennsylvania Ave., NE, North Building, 10th Floor, Washington, DC 20004. Phone: 202-756-3334. E-mail: Pkazon@alston.com.

Carrie Valiant

Lab Compliance, *from p. 1*

"So, what if you use the computer or new technology beyond 'exclusively' and what if that use is valued and paid for? Is that the flip side of the prohibition?" poses Valiant. "These are issues we've been dealing with, especially as new technology comes out."

Technology potentially supplied by labs now goes beyond just computers and fax machines, she notes. There are next-generation technologies that will improve quality and timeliness of results, but the expense often is prohibitive for physician offices.

"The question is, can you apportion the benefits between the two parties so that the technologies can be made more widely available and decrease costs of processing lab services for everybody?" asks Valiant. "I'm not sure there's a clear answer to this, but to my knowledge the OIG has looked at some of these arrangements and hasn't necessarily acted upon them. These are the kinds of issues that are going to be challenging to the industry on an ongoing basis."

Another issue addressed by the fraud alert that continues to be a concern is free managed care testing, notes Valiant. According to the 1994 fraud alert, an out-of-network lab that agrees to perform a physician's managed care work free of charge so the physician will continue to use the lab for nonmanaged care work could be in violation of the anti-kickback statute.

According to the fraud alert, the statute is implicated when the physician's managed care contract incentives or penalties regarding utilization of services results in a financial benefit to the physician from the lab write-off, she explains.

"Currently, a lot of labs are having physicians certify that there is no financial benefit," she says. "Does it work? It's hard to say. This is a very competitive, controversial issue, and it's something labs need to be very careful with. It is unclear to me that the statute is even implicated because physicians frequently don't even know what's in their managed care contracts, so how can [the benefits] be an inducement? But the fraud alert says it, so we have to live with it."

Managing Fair Market Value

According to Valiant, being able to document fair market value of service is also a critical issue, particularly when you're facing a government investigation. "It's way more important to have your fair-market value ducks in a row than to have a 50-page lawyer letter that expounds on theory," she says.

Much of the time there may be no need for an independent third-party valuation of goods or services, she says. Typically, careful documentation added as a memo to a file will be sufficient. "For example, if you're paying physicians hourly rates supported by MGMA standards, putting memos in their files to that effect will probably pass muster, although complicated arrangements probably need more."

It's much better for defense purposes to include contemporaneous documentation at the front-end of the process than to try to recreate it at the back-end when requested by government investigators, adds Valiant. "This is critically important, probably more so than a lot of the other compliance issues you spend your time on," she says.

Among the documents that labs should maintain are signed contracts, time sheets, and descriptions of work performed, and nonprivileged documentation of the rationale for the arrangement.

Separating Law From Lore

One problem that many healthcare providers face is confusion between what is required by law and what is simply a good idea. This confusion can be costly if it leads to legal action, says Valiant.

"If you give an impression that something is a law or a rule when it isn't, it can come back to bite you," she explains. "We see this a lot in our whistleblower cases. There are people running around institutions enforcing 'rules' and 'laws' when they really are just best practices. When compliance is not achieved with those best practices, the whistleblower will file a complaint, and we spend a lot of your time and money proving that it's not a rule or a law." For example, she explains, some healthcare workers are under the mistaken impression that advance beneficiary notices (ABNs) are

Audio recordings of this compliance workshop and all Lab Institute sessions are available for purchase at www.g2reports.com.

required for every insurance claim. In fact, ABNs are required only for services that Medicare may not pay for and only if the provider plans to bill the patient for services provided. If a provider intends to write-off the service, an ABN is not necessary. "You may have an issue if you have too many write-offs, but you don't have to get an ABN for every single claim," explains Valiant.

Another example involves billing Medicare Part B for deeply discounted "bundled" goods. Some people believe "you need a cost to bill Medicare," she says. "That may be true under Part A cost-reporting, but Part B is charge-based, not cost-based, and items that are discounted or bundled or free may fall under a safe harbor."

To avoid potential whistleblower problems, Valiant advises, you must be clear to specify whether a policy is merely a best practice or is actually based on law.

Managing Compliance Matters

What should you do when you have identified a compliance problem in your organization? Generally, it's a good idea first to determine if the perceived issue is really a problem, says Valiant. You may also want to contact the OIG's industry guidance branch to request an advisory opinion.

"You have to be careful what you ask for though because if the OIG says no, you'll have to stop whatever it is that you're doing or thinking about doing," she advises.

Valiant also suggests that healthcare organizations and providers make sure they use the "right door" when approaching the OIG. You can actually bring an investigation on yourself if you request an advisory opinion about behavior you believe to be non-compliant instead of making a voluntary disclosure.

Finally, Valiant notes that providers do not always have to go to the OIG when there is a problem. In some cases, such as when there is a strict financial matter involved, it is sufficient to report the problem and make repayment to the carrier or fiscal intermediary.

Resource

Carrie Valiant: 202-861-1857

RTI To Design Lab Bidding Demonstration

The Centers for Medicare & Medicaid Services (CMS) has selected RTI International (Research Triangle Park, NC) to design and launch a Part B competitive bidding demonstration for independent laboratory services.

The demonstration project is mandated by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 and is to apply to laboratory tests performed by entities without a face-to-face encounter with patients. It excludes Pap tests and colorectal screening tests.

Linda Lebovic, MPH, MT(ASCP), the lab demo's project officer at CMS, says the agency is continuing to accept input and comments from the lab industry on the project. Lebovic spoke during *Lab Institute 2004*, sponsored by Washington G-2 Reports. The conference was held September 29 to October 2 in Arlington, Virginia. Specifically, she said CMS is working on how to define lab services that don't involve a face-to-face encounter.

A technical expert panel will advise the contractor as it designs the demo, Lebovic said. Lab groups, which largely oppose the project, want to be sure they have a say in how the demonstration is set up and run. Alan Mertz, president of the American Clinical Laboratory Association, said during Lab Institute that his group and others in the Clinical Laboratory Coalition definitely "want to be at the table."

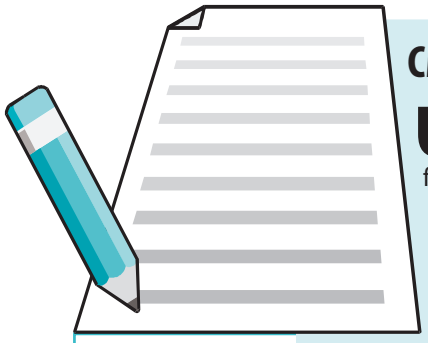
More on the competitive bidding demonstration project for laboratory services is available at *www.cms.hhs.gov/researchers/demos/clinicallabdemo.asp.*

FDA To Issue Guidance On Waived Tests

The Food and Drug Administration (FDA) is expected to publish consensus guidance within the next several months outlining improved criteria for waived tests. The guidance will be based on the recommendations of the Clinical Laboratory Improvement Advisory Committee (CLIAC), which has set up a workgroup on good laboratory practices for waived testing. The workgroup will report back at CLIAC's next meeting in February 2005.

FDA regained authority for CLIA-waived test categorization in April when the Department of Health and Human Services transferred authority from the Centers for Medicare & Medicaid Services (CMS).

A 2002 CMS survey of 897 CLIA-waived labs found that serious quality problems exist in many of the facilities. Of the labs surveyed, 44% had new testing personnel, 8% tested beyond the scope of their waiver certificate, 14% lacked current manufacturer instructions, and 24% did not perform quality control as required by the manufacturer. Preliminary results from a 2003 survey of 1,756 labs show similar findings, according to reports at CLIAC's last meeting, held September 22 to 23 in Atlanta.



for the Record

CMS Modifies Policy on Billing for Purchased Tests

Until further notice, physicians and suppliers must bill their local carrier for all purchased diagnostic tests and interpretations, regardless of where the service was furnished, the Centers for Medicare & Medicaid Services (CMS) instructs in Transmittal 315, issued October 22.

Currently, Medicare carriers must use the ZIP code of the location where a service is rendered to determine both the carrier jurisdiction for processing the claim and the correct payment locality for any service paid under the Medicare Physician Fee Schedule (MPFS). Diagnostic tests and their interpretations are paid under the MPFS and are therefore subject to the same payment rules as all other services under the MPFS. Laboratories, physicians, and independent diagnostic testing facilities (IDTFs) may bill for purchased tests and interpretations. However, under the current jurisdictional pricing rules, these suppliers must bill the purchased test or interpretation to the carrier that has jurisdiction over the geographic location where the test or service is performed.

Since the implementation of carrier jurisdictional pricing edits on April 1, 2004, CMS has received reports that, due to current enrollment restrictions, some physicians and suppliers purchasing diagnostic tests/interpretations are unable to receive reimbursement for these services when they are performed outside of their local carrier's jurisdiction. CMS is temporarily changing the pricing rules that apply when billing for an out-of-jurisdiction area purchased diagnostic service.

Transmittal 315 specifies that physicians and suppliers must bill their local carrier for all purchased diagnostic tests/interpretations, regardless of where the service is furnished. The billing physician or supplier is responsible for ensuring that the physician or supplier who furnished the purchased test or interpretation is enrolled with Medicare and is in good standing. The billing physician or supplier is also responsible for any existing billing arrangement between the purchasing entity and the entity providing the service.

When billing for an out-of-jurisdiction purchased diagnostic service, the physician or supplier must report the address of its facility in the service facility location area of the claim. (For these services only, the place of service is deemed to be the billing physician's or supplier's location, rather than the location where the service actually was performed). When billing for a diagnostic service purchased within the local carrier's geographical services area, the physician or supplier must continue to follow existing guidelines for reporting the location where the service was furnished.

For out-of-jurisdiction purchased diagnostic services only, carriers must use the ZIP code of the billing entity's location to determine both the carrier jurisdiction over the claim and the correct payment locality for the amount payable under the MPFS.

Physicians and suppliers billing for purchased diagnostic services will not be penalized by the Office of Inspector General when they change the service facility location on the claim, even if the location reported on the claim does not correspond with the location where the service was actually performed, says CMS. Transmittal 315 is available at *www.cms.hhs.gov/manuals/pm_trans/R315CP.pdf.*

❖ **Antitrust Scrutiny Continues**: The Federal Trade Commission and the Department of Justice recently issued a 361-page report, "Improving Health Care: A Dose of Competition." The report describes the agencies' current thinking on the application of the antitrust laws and their enforcement priorities in the healthcare industry. It also provides some important new guidance. According to the report, antitrust investigations and enforcement action against healthcare providers will remain a top priority for the agencies. In particular, provider network joint ventures, hospitals, group-purchasing organizations, and insurance and pharmaceutical companies should anticipate continued scrutiny.

❖ **CMS Names HIPAA Director**: Nathan Colodney has been tapped to head the Office of Health Insurance Portability & Accountability Standards at the Centers for Medicare & Medicaid Services (CMS). Colodney, former chief information officer in the Office of the Solicitor in the Department of the Interior, began his job at CMS October 18. He takes over for Karen Trudel, who had been acting director of the office during the last year.

❖ **Hospice Company Targeted**: Odyssey HealthCare, one of the country's largest hospice care providers, is the focus of a False Claims Act investigation by the Department of Justice, the company announced October 18. In a statement to investors, Odyssey said DOJ's civil division notified the company in September that it was investigating Medicare claims submitted by the hospice provider from January 2000 to present. Specifically, the government told Odyssey it is reviewing company conduct in the areas of patient admissions and retention, as well as billing practices. Odyssey said in its statement that it has "a longstanding and ongoing employee training and regulatory compliance program, including a mechanism for employees to alert management anonymously of issues."

❖ **Executive Pay Perks Cut**: Congress in October approved legislation that will enact sweeping changes in the rules governing nonqualified deferred compensation plans. The American Jobs Creation Act of 2004, which is expected to be signed into law by President Bush, is part of a larger package aimed at curtailing abuses that occurred at Enron and other companies in recent years. Nonqualified deferred compensation plans have long been a staple for senior management and officers of both for-profit and tax-exempt organizations. Under the new legislation, deferrals of benefits will still be possible, but under much more restrictive rules.

G-2 Compliance Report (ISSN 1524-0304) is published by Washington G-2 Reports, (a division of the Institute of Management and Administration), 3 Park Avenue, 30th Floor, New York, NY 10016-5902. Telephone: (212) 244-0360. Fax: (212) 564-0465. Order Line: (212) 629-3679. Website: www.g2reports.com

Group Publisher: Perry Patterson. *Managing Editor:* Kimberly Scott, 301-260-0929.