CCH Health Care Compliance LETTER

Volume 11, Issue 8 health.cch.com April 15, 2008

Former drug company CEO indicted on wire fraud, FDCA charges

The former Chief Executive Officer (CEO) of InterMune Inc. was indicted on wire fraud and felony Food, Drug, and Cosmetic Act (FDCA) charges for his role in the creation and distribution of false and misleading information about one of the company's drugs, the Department of Justice (DOJ) announced.

Elements of the indictment. The indictment alleged that, under the CEO's direction, InterMune marketed and sold Actimmune® to treat idiopathic pulmonary fibrosis (IPF), a fatal disease, even though the drug was not approved by the Food and Drug Administration (FDA) as safe and effective for treatment of the condition. According to the indictment, the CEO and InterMune promoted Actimmune® as a safe and effective treatment for IPF to increase sales of the drug and generate revenues and profits from those sales. The cost of Actimmune® for one IPF patient for one year was approximately $50,000, and most of the company's sales of the drug were for the unapproved, off-label use of treating IPF.

The indictment further alleged that the CEO devised a scheme to induce doctors to prescribe, and patients to take, Actimmune® to treat IPF. Specifically, as part of the fraudulent scheme, InterMune issued a press release announcing false results of a clinical trial of Actimmune® for the treatment of IPF. Although the press release stated that the drug "reduces mortality by 70 [percent] in patients with mild to moderate disease," the clinical trial failed. In furtherance of the scheme, the CEO caused a specialty pharmacy to disseminate the misleading information in the press release to more than 2,000 pulmonologists and to patients taking Actimmune®.

The CEO may face up to 20 years in prison, a $250,000 fine, three years supervised release, and a $100 mandatory special assessment for the wire fraud charges; and three years in prison, a $250,000 fine, one year supervised release, and a $100 special assessment for the FDCA violations.

InterMune's settlement. In October 2006, InterMune entered into a deferred prosecution agreement and agreed to pay approximately $37 million to resolve criminal charges and civil liability in connection with the fraudulent marketing scheme. The company also entered into a five-year corporate integrity agreement with the HHS Office of Inspector General.

"Pharmaceutical executives who promote drugs using false and misleading information should not be allowed to hide behind a corporate shield," said Kim Rice, Special Agent in Charge of the FDA's Office of Criminal Investigations, Washington Field Office. She added, "Pharmaceutical companies do not run themselves, and those who engage in criminal conduct will be held personally responsible." ■

DOJ Press Release, March 18, 2008.

Wolters Kluwer Law & Business

Electronic information preservation may reduce complications, costs

Preserving electronically stored information prior to a litigation hold can prevent a lot of headaches, costs, and complications, according to Henry Willett III, Christian & Barton, Richmond, Virginia. "Do not wait until a litigation hold is necessary to learn what information a client has ... that may need to be preserved," Willett said during a March 26, 2008, American Bar Association audio conference.

A litigation hold is a suspension of an organization's document retention/destruction policies to ensure preservation of materials that may be relevant to a lawsuit that has been filed or is reasonably anticipated. Waiting until litigation has been or soon will be filed to become familiar with the scope of an organization's electronically stored information will make it harder to get control of the information and more expensive to take the steps to maintain that information, Willett said.

New civil procedure rules for e-discovery. The December 2006 changes to the Federal Rules of Civil Procedure require that, as part of the initial "meet and confer" to plan discovery, parties specifically address electronic discovery issues, including, for example, what steps counsel and their clients will take to preserve and retrieve electronically stored information and what format they will use for electronic production. "Now there's an affirmative obligation on the parties to discuss potential electronic discovery issues on the front end," Willett noted during a brief interview following the audio conference.

Steps for counsel prior to litigation. Before a claim arises, Willett advised, counsel must become familiar with the information the organization has stored electronically; establish personal contact with key information technology (IT) personnel; and understand what devices, networks, and operating systems the organization is using and where information is stored. "Become familiar with your company's technology," he said. "You need to make sure that you know where to find the information."

Counsel also should review remote workstations. Willett noted that employees may access files through a central server, but cached copies may remain on workstations when the employees are working outside the office.

Early on, the organization's e-mail usage and retention policies should be reviewed. "You need to know how long your company stores e-mails," Willett emphasized. Document retention policies may need to be changed so that materials are neither destroyed too quickly nor retained for too long. "E-mail is in most cases the source of a tremendous amount of information and headaches when searching for, preserving, and retrieving information that can be used in litigation," Willett cautioned, adding that the organization may want to consider policies that limit the scope and use of e-mails.

Steps after litigation hold. Once a litigation hold is deemed necessary, the organization should identify key business and IT contacts, identify all potential custodians of relevant information, and determine the scope of information sources, Willett said. He suggested interviewing the custodians and recording the date of each interview, title of the interviewee, his or her contact information, computer devices used, a brief description of the content, where the information is stored, and dates that the information may have been generated or used.

In conjunction with the interviews, counsel should prepare and distribute a preservation letter to potential document custodians instructing them to take all necessary steps to prevent potentially relevant information from being deleted, Willett advised. The first draft of the letter should be broad and cover any documents that could relate to the potential claims, but, if possible, the letter should be narrowed later to conform to the scope of the litigation hold, he said. "That job is made much easier by the work that you've done on the front end in identifying what potential information is out there."

Counsel should take an active role in litigation, prepare for the discovery conference, and participate in preparation of the proposed discovery plan, Willett emphasized. "It makes a great deal of sense to work with the other side in determining how information will be produced so that resources are not unnecessarily exhausted gathering information in a manner that is not conducive to the ultimate production," he said. He added that counsel should limit discovery and preservation obligations to specific categories of documents and information, as well as certain identified custodians. "The goal of all sides should be to preserve only that information that needs to be preserved and to make sure that the information that's relevant is produced." ■

CCH Washington Bureau, March 31, 2008.

CCH Health Care Compliance Letter

Portfolio Managing Editor
Pamela K. Carron, J.D., LL.M

Coordinating Editors
Susan Smith, J.D., M.A.
Matthew Mann, J.D.
Valerie Witmer, J.D.

CCH Washington Bureau
Paula Cruickshank
DOJ, FTC–John Scorza
SEC–Peter Feltman
Health Law–Catherine Hubbard, M.A.
Tax–Jeff Carlson, Steve Cooper

Designer
Kathie Tingson Luzod

Requests for information about article submission and comments from readers are welcome and should be directed to Susan Smith at susan.smith@wolterskluwer.com, Tel. 847-267-2780, Fax 847-267-2514. Customer service inquiries should be directed to 800-449-9525.

CCH Health Care Compliance Letter is published 24 times a year by CCH, a Wolters Kluwer business, 4025 W. Peterson Avenue, Chicago, IL, 60646. Subscription rate is $305 per year. First-class postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: SEND ADDRESS CHANGES TO *CCH Health Care Compliance Letter*, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A.

CMS faces challenges ensuring reliability of hospital quality data

The issues and challenges related to how hospitals collect and submit quality data to CMS and how CMS ensures the reliability of the quality data submitted was the focus of testimony given by Linda T. Kohn, Government Accountability Office (GAO) Acting Director, Health Care before the Senate Finance Committee on March 6, 2008.

CMS' Annual Payment Update (APU) program requires participating hospitals to submit quality data for calculation of hospital performance on quality-of-care measures. In the APU program, each quality measure consists of a set of standardized data elements. Hospitals determine a value for each data element for all patients, both Medicare and non-Medicare, who have a medical condition covered by the APU program. The values of the data elements consist of the numerical data and other administrative and clinical information that is obtained from the patients' medical records.

Collecting and submitting data. The GAO reported in April 2007 that eight case study hospitals used the following six steps to collect and submit quality data to determine the appropriate value for each data element: (1) identify patients for whom the quality data should be submitted; (2) locate needed information in the medical records; (3) determine the appropriate value for each data element; (4) transmit the data to CMS; (5) review reports to ensure CMS' acceptance of the data; and (6) supply copies of selected medical records to CMS for data validation.

Steps two and three involve complex abstraction, that is, reviewing and assessing all relevant pieces of information in a patient's medical record. Many factors account for the complexity of the abstraction process, including: (1) content and organization of the medical record; (2) variety of techniques used by individuals abstracting the data; and (3) use of hospital staff trained to follow a detailed protocol to extract specified information consistently from Medicare records that have data element values in various sections. The scope of information and clinical judgment required for certain data elements may be represented not by a single discrete piece of information, but rather by a composite of related data and the abstractor's clinical judgment, which is governed by complicated rules.

Frequent changes in the data specifications set by CMS make it important that hospital abstractors note the changes requested and revamp their data collection procedures accordingly. Hospitals generally reported that the amount of staff time required for abstraction increased proportionately with the number of conditions for which the hospitals reported quality data. This was balanced, however, by the clinical performance information hospitals collected on themselves, which they used to track changes in their performance over time.

The GAO's case studies showed that existing information technology (IT) systems help hospitals gather some quality data but are far from enabling hospitals to automate the abstraction process. IT systems offer hospitals two key benefits: (1) improving accessibility to and legibility of the medical record; and (2) facilitating the incorporation of CMS' required data elements into the medical record.

Validating data. CMS has a process for ensuring accuracy but has no ongoing process for ensuring completeness of quality data. To check accuracy, one CMS contractor electronically reviews the data as it is submitted to the clinical warehouse, then another contractor conducts an independent audit by comparing the quality data submitted by each hospital for a sample of five patients per quarter with the quality data that the contractor re-abstracts from the same medical records. The data is deemed accurate if there is 80 percent or greater agreement between the two sets of results. CMS' determination as to whether hospitals have met the accuracy standard, however, was statistically uncertain for some hospitals because of the small number of records examined—five per quarter, regardless of hospital size.

CMS does not have an ongoing process for assessing the completeness of quality data submitted by hospitals. For fiscal year 2008 and subsequent years, CMS is requiring that hospitals attest to the completeness and accuracy of their data quarterly. CMS plans to redesign the data infrastructure and validation process (*e.g.*, by increasing the number of patient medical records sampled from select hospitals) to support a value-based purchasing program. ■

GAO Testimony, GAO-08-555T, March 5, 2008.

On The Front Lines

Exacting a price for audit compliance

by Allan P. DeKaye, MBA, FHFMA, Editorial Advisory Board Member

This article examines why the provider seems to be on a continuous "slippery slope," seemingly always on the precipice of falling into the recesses of fraud and abuse. The article looks at the overwhelming increases in auditor funding and mandates, as well as the diversity of audit areas now being examined. It contrasts this with the best efforts and practices providers have developed and implemented and compares it to the level of resources being consumed to protect and defend itself. Finally, it looks at alternative mechanisms to differentiate the levels of good, bad, and evil (providers), and how much they will need to spend to achieve a state of audit compliance.

I had the privilege of authoring the initial *On The Front Lines* column as this publication debuted on December 7, 1998. The theme of that article, entitled "Additional Documentation Requests and Other Audits—How to Survive," seems an apropos reference to our fast forwarding almost ten years later to today's audit intensive environment. Additional Documentation Requests, or ADRs, as they were known then, are still with us today. Only now, they are joined by their not-so-distant cousins with other acronyms, such as RAC (Recovery Audit Contractor) and OMIG (Office of the Medicaid Inspector General), all descendents of their more respected relative, the HHS Office of Inspector General (OIG).

These relationships are more than symbiotic. In fact, the federal and state partnership now in place in many states portends a new era not only for health care providers—the traditional focus (read: target)—but also for an all encompassing range of organizations from Medicare contractors, to state Medicaid agencies and even insurance plans. Individuals, including providers and other care givers, or those who knowingly and willingly abuse the system, will continue to be subject to investigation, prosecution, and, when convicted, restitution and incarceration. This article examines how the provider, in particular, seems to be on a continuous and perilous slippery slope in the area of protecting itself from committing improper acts in the course of delivering care, and how it can assure both its own governing authority and the government's auditing authority that it is a good corporate citizen.

Tracing the roots from good to bad to evil

The literature is replete with a seemingly endless array of cases of fraud and abuse investigated by federal, state, and local jurisdictions. What have become alarming are the recovery rates and the sheer value of the restitution that appears to be a geometric rather than an arithmetic progression.

During the three-year period from fiscal year (FY) 2005 to FY 2007, the total OIG expected recoveries averaged $3.14 billion per year, exceeding all previous reporting periods and the prior reporting period by 17 percent.[1]

When examined in more detail, the scope of audits has not only continued in the more traditional area of claims submission, but also migrated into reimbursement calculations and cost reporting, which triggers a more intense examination. With the addition of quality based audits (*e.g.*, medical necessity and, eventually, clinical outcomes, etc.), the health care provider is faced with a constant barrage of audits. Preparing for and defending against this ongoing effort (read: attack) could be likened to an army under siege. This becomes an especially daunting task, when even the auditors must show a cost/benefit realization to support the continuation and increasing levels of its funding mandates.

The return averaged more than $1.82 billion in investigative receivables and $1.32 billion in audit disallowances per year. The resultant organization-wide return on investment for the FY 2005–2007 reporting period was $14.5 for each dollar spent in the OIG operating budget.[2]

This article does not seek to portray the provider as above reproach. In fact, the provider has caused its own problems in many respects. Frances J. Serbaroli, Esq. noted, "Fraud is widely regarded as another significant factor in the escalation of Medicaid costs." He added, "[T]he...OIG has estimated that 10 [percent] of all health care expenditures are attributable to fraud."[3] Additionally, providers have been subjected to whistleblowers calling attention to uncorrected problem areas.

The United States has intervened against three New Jersey hospitals in two whistleblower lawsuits alleging that the hospitals defrauded Medicare...by inflating their charges...to obtain enhanced reimbursement.[4]

Hospitals are not alone, as the federal and state governments cast a wide net to identify fraud in other health care areas. For example, "New York Attorney General (AG) Andrew Cuomo is conducting an industry-wide investigation into a scheme by health insurers to defraud consumers by manipulating reimbursement rates."[5] The cost of this effort will be discussed in later sections, but first, it is important to understand how the audit environment has changed.

Arming the auditor with technology and resources

In an earlier, simpler time, a claims audit would rely on a sample selection from a hospital's detail trial balance (or listing of all of the claims that were billed), with every "X" accounts selected to test for one or more payment or claims condition. Today, with the data mining capabilities that exist, notably for the two largest payers, Medicare and Medicaid, the provider is faced with the confluence of targeting audits that may encompass as much as 70 percent (or more) of its service delivery volume. Adding to that is the myriad of regulations, many of which dictate the audit elements that, if found to contain errors, may subject the provider to liability, recoveries, and penalties under the False Claims Act. The provider needs to establish proactive editing software to screen for a countless number of conditions to which it must adhere.

Although many providers will employ a combination of pre- and post-claim editing from encoders, claims scrubbers, and clearinghouses, these tools cannot provide an effective levee system if the underlying operational workflows are flawed, ineffective, and inefficient. The auditor is now able to supplement the more traditional review of policies and procedures with a more exacting targeted list of claims and medical record requests to validate the appropriateness of a claim across many dimensions.

As was the case with the ADR reviews, the audits placed a burden of proof on the provider to demonstrate documented event occurrences, but also added a timeline for producing these supporting elements. This enabled auditors to gain in efficiency, as it reduced the need to deploy teams of staff to the field. Operations could be centralized, and productivity could be increased multifold. But these gains pale in comparison to the infusion of resources. Increases in staffing are most evident in New York's Federal-State Health Reform Partnership (F-SHRP) effort.[6]

In addition to being one of the first states to be part of the RAC demonstration initiative, along with California and Florida, New York's F-SHRP program has demonstrable recovery targets that, if not achieved, will result in the federal government taking back the funding it has advanced to offset the state's added investment in staff resources and technology. The addition of this covenant makes "Auditing in a New York State of Mind"[7] a gaming proposition for providers. It is unlikely that the state will want to be on the short end of a funding situation. The fact that New York will subcontract some of its audits to entities that will be paid on a contingency rate basis (*i.e.*, a percentage of recoveries) is a daunting proposition.

At an industry trade association meeting, New York's Medicaid Inspector General, James G. Sheehan made the following points that seemed to signal to providers that the audits would not necessarily be "kinder and gentler," but that they would be "fair and firm." Sheehan made the following points that seemed to back up this premise. New York's OMIG would differentiate audit findings that tended to be the result of "payment billing errors" and not committed with fraudulent intent. For these audit findings, the state would expect restitution, but not necessarily penalties. Sheehan added, however, that when there was evidence of fraud, the full extent of prosecutorial remedies would be used. Perhaps the audit element that signaled a more invasive approach was the involvement of provider governance and the role it plays in oversight and correction. With the implementation of the F-SHRP initiative, the OMIG was laying down the gauntlet with three challenges that providers could expect in every audit:

(1) *Notice.* Caveat emptor, or "let the provider beware," it must know the conditions of participation for all payers. In effect, providers are on notice that they must meet every condition of participation.
(2) *Warning.* In effect, F-SHRP is the "shot fired across every provider's bow," sort of a "Miranda warning" for providers.
(3) *Failure to act.* Whether at the departmental, administrative/management, or board level, inaction would not be a defense, but an admission of wrongdoing.[8]

Combining RAC and OMIG audits, health care providers in New York are subjected to many audits per month. Each new audit could cover another discipline, with new time tables for administrative compliance and the reality that many audits will be ongoing in various stages at once.

Advancing compliance through provider safeguards

While most providers will have corporate compliance plans, the key question to be addressed is how effective these plans are in detecting errors and preventing them from being perceived as fraudulent in nature. The characteristics of effective compliance programs are likely to include some or all of the following:

(1) *More than paper compliance.* This is a broad-reaching statement that says "that the provider does what it says" in its compliance plans.
(2) *Staff awareness and training.* This is a staple ingredient of compliance plans that must demonstrate that staff receives a compliance introduction, usually at a new employee orientation, but also, at a minimum, at annual retraining that emphasizes important operational areas where vulnerability and risk are more likely to occur. Best practices likely incorporate more frequent types of training, including, but not limited to, in-service "mini" sessions, staff meetings, departmental memoranda, online tutorials, and periodic formal assessments.
(3) *Charge, coding, and claim editing.* Effective "automated" and "manual" editing throughout the revenue cycle accounting process is a fundamental building block of a strong compliance program. To the extent that these edits combine both "blocking" and "warning" capabilities that a potential problem, inconsistency, or error exists, the provider will have an opportunity before generating a claim to remedy any deficiency. When any type of edit occurs with frequency, a

provider's ability to investigate and remediate the processes that caused the error(s) in the first place will be an important cornerstone of effective ongoing compliance monitoring.

(4) *More than just a corrective action plan.* All too often, corrective action plans are viewed as just a response to an audit. Despite initial efforts to correct noted deficiencies, long-term adherence to these efforts has had tendencies to falter. With this fact in evidence, audit entities have added follow-up reviews to measure long-term adherence to these plans. As a result, providers often may have repeat deficiencies. Providers who can implement solutions that lead to more permanent remedies are better able to demonstrate that their actions are both sincere and effective.

(5) *Combining clinical and administrative resources.* With the increasing indications that audits will be focusing on clinical outcomes, medical necessity, and quality care delivery, providers who have established effective utilization review and case management programs will find themselves better able to adapt to these types of audits. If they have been able to create denial databases that track the status of admission reviews and continued stay reviews, and establish the effectiveness of their rebuttals and supporting documentation and appeals, then they have in place the infrastructure to tackle the next phase of audit emphasis.

(6) *Conducting risk assessments.* Each year, the OIG issues its workplan identifying areas of concern and attention for the coming year. Many providers use this document as a guide to add risk assessment studies to see if there are potential vulnerabilities. The ability to maintain its defense of existing areas of concern while evaluating new threats is an example of a strong compliance plan at work.

(7) *More than just HIPAA.* While HIPAA compliance is clearly an important area of concern, too many providers seem to have devoted more energy to this area, while foregoing some other core elements of compliance.

For those providers who have faced restitution or entered corporate integrity programs, these steps likely have become part of a more permanent corrective action program. Similarly, self-reporting of material problems can be viewed as a proactive approach that further demonstrates a provider's awareness and sincerity in adhering to its own compliance program.

"Voluntary disclosure offers certain benefits, including substantially lessening the potential civil, criminal, or administrative liabilities," Serbaroli noted. He went on to caution, however, that "before a provider chooses to self-disclose any improprieties to the federal government, it should first consult with counsel and then perform a thorough risk/benefit analysis."[9]

The problem for providers is funding all of these defensive and preventive initiatives in the face of decreasing reimbursements from governmental, managed care, and private payers.

Providers: Winning the battle, losing the war

Surviving today's audit intensive environment will require more than just doing it correctly. For most providers, there will be a need to devote more resources to meet the administrative demands of complying with data requests and time frames, which, if not met, can result in adverse determinations. Many providers, however, will not be able to devote the added audit management resources, often having to rely on line managers and staff to handle those functions in addition to day-to-day responsibilities.

These increasing audits also come at a time when providers have reduced internal audit resources, again sometimes turning to outsourcing these internal audit functions to outside firms or organizations. As organizations wrestle with resource allocations in a time of decreasing reimbursement, they will still need to deal with these added audit risks.

Another area that is consuming administrative resources relates to a provider's adherence with financial assistance and bad debt and charity care determinations. Many hospitals, in particular, recently have gone through a period of revising their policies and procedures to conform to (or go beyond) the standards being advanced by national trade associations by making their application processes more available to the public, as well as making their pricing for services transparent.

Advantage auditors: In search of a better way

Leveling the playing field for providers has become more difficult. One key element can be the use of a provider's own data. A provider's ability to effectively "data-mine" its own claim information, as well as process information, can go a long way to supporting itself in audit defense. A few years ago, providers began to find that an unintended benefit of document imaging systems was the ability to retrieve account information or supporting documentation that was captured in scanned forms. Even now, as providers begin to expand the development of the electronic medical record (EMR), they have the potential to produce clinical records for audit support. This will prove invaluable in responding to the time frames these new audits impose.

However, producing electronic or scanned images that confirm the absence of documentation for a test that was supposedly performed or charges that were misapplied or not posted correctly to a claim will only facilitate providers responding with essentially a *nolo contendere* (or no contest) plea that will result in negative audit findings. While many provider institutions are self-funding EMR development, there seems to be a wide-range of grant and other funding sources (including government support) available. EMR development alone will not be an absolute audit defense. Sound workflows, strong editing, and well-trained staff also will need to be in the mix.

There was a time in the early rollout of corporate compliance plans that the compliance department was exempted from the scourge of annual budget cuts. That time has past. Providers will find, however, that they will need to find the funding and support not only to improve, but also to be able to defend themselves.

Determining the price for achieving reform and redemption

One area that should be explored and reexamined is the return to some form of "Medicare's Presumptive Waiver of Liability." In an earlier time and place (circa 1980's), a provider could meet this "condition of participation" by demonstrating that it knew when a "service was covered." While advance beneficiary notices have replaced the concept of providing beneficiaries and providers with a more formal way to advise a patient when services are not covered, there were protections afforded providers exempting them from penalties when they could demonstrate their knowledge. Perhaps what is now needed is for a provider to be able to demonstrate by its performance on successive OIG, OMIG, or RAC and equivalent audits that it should be exempt from (this type or selected) audits for some period of time.

This concept applies for other types of risks, namely insurance policies. Automotive policies, for example, add risk for poor performance (*i.e.*, accidents, violations, etc.). Why not establish that if a provider passes an audit (with some demonstrable criteria set and agreed to) that it would earn a respite from audits. On the other hand, there has been concern with overzealous auditors, especially those with contingency arrangements, conducting overreaching studies that did not yield results, but cost the provider much in the way of defending itself.

This contingency fee or bounty mechanism sets some incentives for these auditors to be overly aggressive and to make questionable decisions in their favor by denying claims.[10]

These remarks have surfaced elsewhere, but in California, these types of rebuttals led lawmakers to consider placing a moratorium on RAC audits. The added scrutiny seems warranted.

The ire of California lawmakers was raised last summer when the California Hospital Association complained that the auditing company selected to review old Medicare payments in the state was targeting claims submitted for the care of patients who had undergone knee and hip replacement surgery. The denial rates have been more than 90 percent of the claims reviewed.[11]

With this type of audit scrutiny, the Vice President for Financial Services at the Florida Hospital Association, Kathy Reep, noted that "internal auditors are starting to demand that hospital administrators adjust their budgeting forecasts in anticipation of future claim denials."[12] This would lead back to the New York OMIG's intent to start holding Boards of Trustees accountable, so the audit responsibilities of reporting to the Board will need to take on an even more significant role.

To achieve a better audit defense, a provider might consider investment in some or all of the following positions:

(1) *Chief audit defender (CAD).* This position would be in direct administrative and clinical control of the various audits. (Note: This would be different than the traditional internal auditor (IA) role, as the IA, if it still exists in an organization, would seemingly have the responsibility for uncovering problems, while the CAD would take on the organization's defense once an external audit presented itself.) This individual could be an attorney, physician, administrator, or senior manager.

(2) *Audit support staff.* This could be comprised of a cadre of staff well versed in finance (*e.g.*, patient financial services background), clinical (*e.g.*, utilization review/utilization case management, and could be a registered nurse or a physician), and coding (*e.g.*, a credentialed coding professional (RHIA, CCS, etc.), as coding makes up a large part of the audit), and an information technology professional to provide the data mining support.

This is likely to be a costly proposition (with an initial annual estimate of between $300K–$500K per year, including fringe benefits), depending on the size and complexity of the facility, and does not include the other compliance costs associated with annual training and other existing compliance activities already in a budget. In the same way that the 2009 OIG budget request showed its $14.5 dollar to one payback, however, providers may well have to spend more to justify protecting their scarce resources simply to perform their care delivery mission.

Allan DeKaye is President and Chief Executive Officer of DEKAYE Consulting, Inc. His firm assists health care clients with financial, compliance, and operational issues. He is a frequent speaker at national conferences, and is author/editor of The Patient Accounts Management Handbook (Aspen). Mr. DeKaye also is a member of the CCH Health Care Compliance Editorial Advisory Board. For more information: call: (516) 678-2754; write: dkconsult1@aol.com; or visit: www.dekaye.com.

1 Office of Inspector General (OIG), FY 2009 Justification of Estimates for Appropriations Committees, at 12.

2 *Id.* at 12.

3 Francis J. Serbaroli, Esq., *New York Declares War on Medicaid Fraud*, 238(105) N.Y.L.J. 1 (Nov. 30, 2007).

4 *DOJ Press Release*, "United States Joins False Claims Act Cases Against Three New Jersey Hospitals," Jan. 24, 2008, *at* www.usdoj.gov.

5 "NY Attorney General Investigates health insurers' fraud scheme," *Health Care Compliance Letter*, Vol. 11, Issue 5, March 4, 2008.

6 "New York Federal-State Health Reform Partnership Section 1115 Demonstration, known as F-SHRP, provides that New York State will undertake significant reforms to promote efficient operation of the State's health system. Under F-SHRP, the Federal government will provide funding up to $1.5 billion (up to $300 million per year) to the State for specific designated expenditures. However, Federal funds are conditioned upon the State meeting milestones and generating saving sufficient to offset the Federal investment." *See* http://www.cms.hhs.gov/MedicaidStWaivProgDemoPGI/downloads/New%20York%20FSHRP%20Fact%20Sheet.pdf.

7 With apologies to Billy Joel ("New York State of Mind").

8 Adapted from the author's attendance at James G. Sheehan's presentation to the Metropolitan New York Healthcare Financial Management Association's (HFMA's) 49th Annual Joseph A. Levi Institute, Feb. 29, 2008.

9 Francis J. Serbaroli, Esq., *Voluntary Disclosure of Medicare Fraud by Providers*, 237(104) N.Y.L.J. 1, 1-2 (May 31, 2007).

10 David Whitney, "Anxiety rises over Medicare audit program," SACRAMENTO BEE, Nov. 26, 2007, at 1, *available at* http://www.sacbee.com/111/v-print/story/520053.html (remarks attributed to Don May, AHA Vice President for Policy).

11 *Id.* at 2.

12 *Id.*

Quality of Care

CMS posts new quality, price, patient experience of care information

CMS has posted new survey information on its Hospital Compare Web site to help consumers make decisions about the quality and value of the health care available to them through local hospitals. Consumers now have access to quality information, patient satisfaction survey information, and pricing information for specific procedures.

The Hospital Compare Web site currently provides information on 26 quality measures, which include process of care and outcome measures. Process of care measures report how well a hospital provides care, and outcome measures report the results of that care.

Recently, CMS added ten new patient experience of care measures. These measures are part of the Consumer Assessment of Healthcare Providers Hospital Survey (HCAHPS), which was a collaborative effort by CMS, the federal Agency for Healthcare Research and Quality, and the Hospital Quality Alliance. HCAHPS is the first national, standardized, publicly reported survey of patient perspectives on care provided during hospital stays.

More than 2,500 hospitals nationwide have been collecting information from a random sample of discharged patients who were treated for various conditions between October 2006 and June 2007. The patients were asked about their experiences of care, including responsiveness of hospital staff and pain management, and how they rate the hospital overall.

Two pediatric asthma measures will now be posted on the Hospital Compare Web site, and CMS plans to add an additional outcome mortality measure for pneumonia this summer.

The new pricing and volume information available on the Web site was derived from surveys of acute care hospital payments Medicare made for treatment of beneficiaries with certain illnesses from October 2005 through September 2006. Information about the cost of care will lead to more informed decision making and, ultimately, improvement in beneficiaries' health and the long-term financial health of the Medicare program. ■

CMS Press Release, March 28, 2008.

In the News

E-prescribing rules promote efficiency, safety

A new e-prescribing regulation (*Final rule*, 73 FR 18918, April 7, 2008) will lead to increased use of lower-cost generic equivalents and more efficient communication between physicians and pharmacies, according to CMS. The rule establishes Medicare Part D e-prescribing standards for four types of information: formulary and benefits; medication history; fill status notification; and provider identifier. The standards will apply to all Part D sponsors, as well as prescribers and dispensers that electronically transmit prescriptions and related information about Part D covered drugs for Part D eligible individuals. Providers, dispensers, and other prescribers are not required to implement e-prescribing, but those who do must comply with the new Medicare standards. "Establishing [e-prescribing] standards...will help pave the way for widespread adoption of e-prescribing throughout the medical community. Broader use of e-prescribing offers beneficiaries safer and more efficient care at lower costs," HHS Secretary Michael Leavitt said. The new e-prescribing standards will be effective April 1, 2009.

CMS Press Release, April 2, 2008.

U.S. joins case alleging kickbacks for cardiac services

The United States intervened in a *qui tam* suit accusing The Christ Hospital, The Health Alliance of Greater Cincinnati, and The Ohio Heart Health Center of defrauding federal health care programs by engaging in a scheme to provide cardiologists improper financial incentives in exchange for generating revenue for the hospital. The law suit alleges that between at least 1999 and 2004, the cardiologists were allocated time at the hospital's outpatient cardiology testing unit based solely on the amount of coronary arterial bypass graph procedures and catheter lab revenues generated by each cardiologist or cardiology group during the previous year. Many of these procedures were billed to and paid by Medicare, Medicaid, and other federal health care programs. U.S. Attorney Gregory G. Lockhart said, "Our office chose to intervene because we believe this case is critical to protecting the integrity of the federal health care benefit programs."

DOJ Press Release, April 1, 2008.

Drug company settles off-label marketing claims

Otsuka American Pharmaceutical Inc., the American subsidiary of Japanese pharmaceutical manufacturer Otsuka Pharmaceutical Co., Ltd., has agreed to pay more than $4 million to resolve allegations of off-label marketing of its drug Abilify®. Otsuka developed Abilify® in Japan and entered into an agreement with Bristol-Myers Squibb (BMS) to copromote sales of the drug in the United States. In September 2007, BMS entered into an agreement with the government to resolve allegations that BMS had improperly promoted Abilify® for off-label uses. (*See Health Care Compliance Letter*, Vol. 10, Issue 21, Oct. 16, 2007). The Otsuka settlement resolves similar allegations that Otsuka knowingly promoted the sale and use of Abilify® for pediatric use and to treat dementia-related psychosis, even though the Food and Drug Administration had not determined the drug to be safe and effective for such uses. Otsuka also entered into a corporate integrity agreement with the HHS Office of Inspector General as part of the resolution of the government's claims.

DOJ Press Release, March 27, 2008.