CCH Health Care Compliance LETTER

Volume 9, Issue 10 health.cch.com May 15, 2006

Corporate Governance Update

The *CCH® Corporate Governance Guide for Health Care* has been updated to reflect the impact of the Deficit Reduction Act of 2005 on compliance programs, changes in the U.S. Sentencing Guidelines related to waiver of attorney client privilege, and activities related to nonprofit hospitals.

Wolters Kluwer Law & Business

Experts advise on privacy complaints, OCR investigations

by Catherine Hubbard, M.A., Contributing Editor

As a privacy officer, you receive a complaint. What do you do?

Focus on the complainant, promptly notify the proper parties, review access to protected health information (PHI), examine the internal investigation file, and develop a plan of action for responding to the Office of Civil Rights (OCR), Phyllis Granade, a shareholder with Carlton Fields, P.A., Atlanta, Georgia, advised during an April 21, 2006, teleconference sponsored by the American Health Lawyers Association.

Responding to the complainant. A privacy officer's first step, according to Granade, is to focus on the complainant to ensure that the individual understands that you have accepted his or her complaint, will treat it the same as any other complaint, and there will be no retaliation toward him or her. In addition, assure the individual that you will:

- investigate the complaint promptly,
- document your findings,
- do everything reasonable to prevent further misuses and disclosures of his or her PHI (assuming a violation),
- take appropriate actions against the at-fault workforce,
- respond to him or her regarding the outcome of the investigation, and
- take appropriate steps to prevent similar events in the future.

Privacy officers should avoid any action toward the complainant that might appear retaliatory, Granede said. Marc Goldstone, an attorney, added that current employees who have filed a complaint "should be handled with kid gloves."

Next steps. Privacy officers should immediately notify legal and compliance departments or officers or outside counsel after receiving a complaint, Granade said. The privacy officer should then:

- review records of access to PHI, including audit trails of electronic PHI for access, edits, copies and printing;
- interview the workers who are implicated; and
- review the PHI disclosed and consider the likelihood of identity (ID) theft.

Granade noted that state ID theft notification laws may require the organization to notify individuals if their PHI has been misused or disclosed.

Responding to OCR. After receiving a letter from the OCR regarding a complaint, Granade recommended that privacy officers notify the compliance or legal departments, then look at the internal investigation file and refresh their memory of the complaint and the findings.

continued on page 2

Privacy officers should develop an action plan for responding to the OCR, Granade said. They should confirm whether the use or disclosure occurred and, if it did, whether it was permitted by Health Insurance Portability and Accountability Act of 1996 (PubLNo 104-191) (HIPAA).

Privacy officers should then prepare a draft response explaining the facts, their analysis under HIPAA, and conclusions, she said. The fact portion of the analysis should include a description of the acceptance of the complaint if it was filed internally, the covered entity's investigational efforts and findings, enforcement efforts and sanctions, and the covered entity's "wrap up" response to the complainant, she added.

The OCR will ask for several documents, including primary investigation materials, audit trails, and interview notes. Privacy officers should consider carefully what to provide, according to Granade. Prior to handing materials over to OCR or having substantive discussions with investigators, officers should clear all materials and conversations with the compliance or legal departments or outside legal counsel. "You have to be very careful what you provide," she said.

Privacy officers also should keep communications with the OCR professional and courteous, Granade stressed. If the OCR investigator is using his or her personal e-mail address to discuss a complaint, ask to use his or her HHS e-mail address. "Don't respond to the personal e-mail address of an HHS investigator, such as yahoo.com or hotmail.com, only respond to the investigator on paper or at an 'hhs.gov' e-mail address," she recommended.

OCR investigators may request action by the facility that is not required by HIPAA, Granade noted. "Check that what they're asking for is actually required by HIPAA," she said. She also suggested considering whether the requested action is appropriate to the circumstances.

Privacy officers should be resigned to a potentially long investigation. "Even complaints that, to us, have no basis in fact can take weeks or months for OCR to resolve," she said.

Avoiding CMPs. Avoid admitting a violation, she stressed. "The last thing you want to do is flat out admit that you violated the law," Granade said. "If you admit a violation, the Secretary [of HHS] has to file a civil monetary penalty." Goldstone noted.

Gerald "Jud" DeLoss, general counsel to Fairmont Orthopedics & Sports Medicine, P.A., noted that the Secretary may not impose a CMP if the covered entity had no knowledge of the event, if the covered entity would not have known using reasonable diligence, and if a violation was the result of reasonable cause, not willful neglect and corrected within 30 days. These affirmative defenses, which can be raised at any point during the administrative process, provide "excellent opportunities" to reduce or eliminate a CMP, he said.

"These are great things to say to the government," said Goldstone, adding that it's possible to reduce the penalty to $1. "If you have enough mitigating factors, you can get the CMP down to a reasonable amount," he said.

Even if the CMP ends up only $1, however, the Secretary has to notify the public. "This is something else for us to worry about," he said, noting that a competing hospital may use that information to claim that PHI at their facility is more secure.

Steps for prevention. To prevent complaints, organizations should raise sensitivity and awareness through training and education, encourage internal complaints, and raise awareness of HIPAA pitfalls by incorporating, if possible, identified complaints into ongoing training at the facility, Granade said.

In conclusion, Granade emphasized the importance of documenting everything related to the complaint and keeping the documentation for at least six years.

The advice is particularly important in light of the recent HIPAA enforcement final rule, which extends CMS' authority to impose CMPs. Under the rule, if the Secretary finds in a notice of proposed determination that a covered entity has violated an administrative simplification provision, he will be required to impose a penalty unless the entity establishes an affirmative defense. The final rule took effect on March 16, 2006 (see ¶700,006). ■

CCH Washington Bureau, April 21, 2006.

CCH Health Care Compliance Letter

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

Coordinating Editors
Susan Smith, J.D., M.A.
Stacey Fahrner, J.D., M.P.H.

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

Designer
Laila Gaidulis

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.

IG, other officials discuss use of enforcement tools

by Susan L. Smith, J.D., M.A., Contributing Editor

The Office of Inspector General (OIG) has a "broad tool box" that can be used as a means of enforcement of criminal and civil laws, including exclusion and civil money penalty (CMP) authority, but the tools must be used effectively, Daniel Levinson, HHS Inspector General (IG) told an audience on April 24 at the opening session of the Health Care Compliance Association's 10th Annual Conference in Las Vegas.

Corporate Integrity Agreements. The first tool, Levinson addressed was the Corporate Integrity Agreement (CIA), which he labeled "a bridge over troubled waters." The CIA is an alternative to exclusion, he said. To the extent providers are honestly attempting to do the right thing, OIG will waive the exclusion. It will use the CIA as a "lynch pin" to keep organizations with problems included in federal health care programs. It is critically important for providers to take CIAs seriously, Levinson said. If a provider breaches the CIA, the provider may be excluded, he added.

OIG has received positive feedback from organizations working under CIAs, Levinson noted. Organizations have taken positive steps toward strict compliance and have appreciated OIG's professionalism. An important element of a successful CIA is keeping the lines of communication open, according to one provider's comments.

Larry Goldberg, Principal Deputy IG spoke about the exclusion of South Beach Hospital in Miami, explaining that South Beach was excluded for noncompliance with its CIA. Goldberg said that the hospital never gave the CIA serious attention.

Among the failures identified were (1) its communication with OIG was poor, (2) it never implemented the CIA requirements, (3) the compliance officer never got a copy of the CIA, (4) the compliance committee never met, (5) there was no independent review organization, (6) employees were not educated, (7) employees were not screened, (8) reports were not timely or complete, and (9) the hospital did not take OIG's calls. The repeated flagrant violations represented a material breach, Goldberg noted. The hospital was given 30 days to cure the violations and presented a plan of correction with a timetable; however, the hospital did not comply with its own plan.

Goldberg said that the OIG expects full compliance with a CIA and expects hospitals or other entities to communicate with OIG. Further, the hospital must instill a culture of compliance within its organization.

Self Disclosure Program. The Provider Self Disclosure Program (SDP) also is an effective vehicle for compliance efforts. The SDP was initially set up in 1998 as a mechanism for providers to investigate, quantify, and resolve potential health care fraud matters. Generally, self-disclosure leads to a less restrictive three-year certification of compliance agreement rather than a corporate compliance agreement, which last five years and requires an independent review organization to conduct and verify audits or claim reviews.

OIG issued an "Open Letter" on April 24, to encourage providers to use SDP to resolve conduct that may result in CMPs for physician self-referral and anti-kickback violations. The open letter specifically focused on situations involving a financial benefit knowingly conferred by a hospital upon one or more physicians.

Traditionally, self-disclosure has been thought of as evidence of an effective compliance program. According to Levinson, provider liability falls along a continuum. When an organization follows the SDP, the multiplier is at the lower level of the continuum. The hope is to settle at the lower level of the continuum, Levinson said.

Other tools. Other tools that OIG uses to help organizations with compliance include Special Advisory Bulletins, Compliance Program Guidances, and Advisory Opinions. These tools are used to overcome the complicated and complex problems that organizations face. When used effectively, they make a huge difference to the program and beneficiaries, Levinson said. ■

CCH Chicago Bureau, May 1, 2006.

OIG Open Letter, April 24, 2006, Health Care Compliance Reporter, ¶530,391.

On The Front Lines

A systems management approach to compliance: Sigma, ISO and the R.O.P.E. System

by Neil B. Caesar, J.D., Contributing Editor

Most healthcare organizations treat their compliance programs as a distinct set of policies, protocols and actions separate from the rest of the organization's operations. In many ways, however, compliance activities work best when integrated into a healthcare organization's operations generally. The pathway to this integration is blazed by applying the tools and concepts of "systems management" to the area of regulatory compliance.

"Systems management" is a concept with many varied definitions, but for the purposes of this article systems management is a process that assesses, manages and improves operations. A formal systems management approach has been utilized by some healthcare organizations for several years. I have found, however, little or no application of these concepts to the area of regulatory compliance. While some compliance programs and compliance officers do embrace and utilize certain systems management concepts, this usually reflects the strengths and preferences of the individual compliance officers, rather than any formal implementation of acknowledged principles.

I have learned that many of my long-standing ideas about compliance and compliance programs are uncommon. I advise my healthcare clients that regulatory compliance programs require them to care primarily about those laws, regulations, and reimbursement rules that affect the way they operate. I advise my clients that compliance issues are in many ways subordinate to operational issues and that synergy could be created if compliance protocols were integrated into general policies and procedures. Among other benefits, an integrated approach would enable personnel to focus on whether the healthcare organization's operational systems are running properly, regardless of whether defects in the systems reflect compliance problems, personnel problems, funding problems, technology problems, or otherwise. Many of my clients embrace this philosophical approach, and many do not. Perhaps I am a compliance Cassandra, shouting "truth" into the wind, alone and unheard.

Several years ago I discussed my unconventional approach with the chief executive officer (CEO) of an accreditation organization. "But, Neil," replied my friend, "all you are doing is applying systems management concepts to compliance." "Systems management?" I replied. "What's that?"

From that moment, I began learning that there was a world of formal concepts, tools and structures addressing how businesses can evaluate and improve their operating systems. I learned that my ideas about compliance were grounded in long established systems management concepts. My lonely soapbox now lay on larger systems management bedrock. Not only have these tools been used since the mid-1980's, they have been created based on ideas used extensively in other industries for generations. I discovered, however, that while some healthcare organizations embraced systems management tools for certain aspects of operational assessment and improvement, there was very little evidence that anyone was applying these concepts to healthcare regulatory compliance programs.

The concepts in this article are offered to pique your interest. By understanding systems management principles and methodologies and their application to compliance programs, we can identify the synergies that arise from adding compliance programs into larger systems management tools. By observing examples of the overlap between systems management concepts and compliance concepts, we can assess objectively the possibilities of an integrated approach toward compliance, including my current approach, the Risk Overload Prevention and Elimination (R.O.P.E.) System. The R.O.P.E. system is the Health Law Center's customized application of systems management tools to healthcare regulatory compliance.

Integrated Compliance

Most healthcare organizations treat their compliance programs as a distinct set of policies, protocols, and actions that operate separately from the rest of the organization's operations. Common wisdom suggests that this separateness is necessary to ensure access at all levels within the organization and accountability for its participants as well as to emphasize the importance of the program.

In many ways, however, compliance activities work best when integrated into a healthcare organization's operations generally. Compliance policies can be more practical when they reflect actual operational realities. Rules and requirements can be embraced more easily by personnel when they are integrated into protocols that personnel currently follow (or should follow). Investigations can be less intrusive when

they focus more easily on identifying systemic problems within the operational activities that led to the compliance problem.

The pathway to this integration is blazed by applying the tools and concepts of "systems management" to the area of regulatory compliance. These include the International Standards Organization (ISO) 9000 system for objective assessment and quality improvement tools such as the Baldridge Award, Total Quality Management (TQM), and Six Sigma. Any one of these tools can enhance a compliance program tremendously because they focus on continual improvement and enhanced value for any operational system to which they are applied.

The merits of integration are worth considering from several perspectives. First, healthcare organizations must create a logical, cohesive system to run their compliance activities. Compliance and audit committees; compliance and privacy officers; and education, investigation, and monitoring protocols are just some of the components that may be part of a compliance system. Each has its separate functions; each must fit within the whole system. In this regard, a compliance system shares many operational similarities to the organization's other systems, viewed from such perspectives as information gathering and dissemination, research/investigation and problem solving, accountability/approvals, and so forth.

Second, a compliance program must draw on the healthcare organization's general resources to roll out its initiatives, and operate the program's ongoing monitoring and auditing functions. Thus, there is a natural integration between the organization's compliance program and its other operational systems.

Third, every organizational system, including a compliance program, operates from a set of rules or procedures specific to that system. In many respects, it does not matter whether the reasons for a particular rule are driven by human resource needs, financial constraints, or compliance requirements. The end result is the same in terms of applying the system specific rules or procedures to a particular problem or activity.

Further, if a compliance program integrates the organization's need to comply with outside laws, regulations, and reimbursement requirements into a broader, "best practices" system, compliance can be evaluated with reference to the organization's general rules of operation as opposed to the system specific rules of operation. This allows the healthcare organization to implement the best method for providing ongoing assessment and improvement. This can be a far simpler and more focused approach toward monitoring compliance.

Viewed from this "best practices" perspective, compliance activities can address how to operate practically, why these operational decisions makes sense, and who should be in charge of implementing and monitoring each aspect of these activities. An integrated approach allows a healthcare organization to delegate supervisory responsibility with reference to each operational activity, with the regulatory overlay being much less isolated. When one element of the activity is not working correctly, the dysfunction may affect regulatory compliance, but it also may affect the efficient (1) distribution of information, (2) use of personnel, (3) spending, and (4) any other organizational goals. Regardless of the effect of the problem, the causes of the problem are assessed through investigation and analysis; the implications of the problem are identified through observation and extrapolation; and from these efforts an appropriate solution is implemented.

Approaches

Systems management initiatives utilize a variety of tools for maximum effectiveness. These tools are often themselves "systems" of a sort, designed to allow an organization to gather and assess information efficiently and implement changes effectively.

ISO 9000

In some ways, the foundation upon which a systems management program can be built lays on the ISO 9000 Quality Series Initiatives. These initiatives were developed by the International Standards Organization (ISO) to document and improve work quality in manufacturing processes. The idea was quickly adopted in other areas of business. The ISO System enables a company to identify what work is performed and how it is performed to ensure that the work maintains an appropriate level of quality. It is an excellent starting point for any systems management initiative. The ISO initiatives do not correct problems or find their root causes; however, problems can be documented very effectively. This feature of the ISO initiatives can be invaluable in assessing and fixing problems. Because the ISO initiatives can assist tremendously in compliance efforts, it is surprising that there has not been a concerted effort by healthcare organizations to embrace this tool in the compliance context. My own integrated approach to compliance, the R.O.P.E. System, is based in the ISO approach.

A compliance program that utilizes the ISO initiatives will not limit its focus to identifying and teaching state and federal laws, regulations and directives that shape the healthcare organization's compliance policies. Rather, the ISO approach to compliance captures as accurately as possible how the healthcare organization implements each of its policies and protocols. For example, specific processes and protocols as diverse as coding claim submission and entering into joint venture agreements could be assessed using a single approach. The compliance officer could then monitor these activities from one perspective, while the financial, clinical and marketing officers monitor from their perspectives.

The ISO approach offers some decided advantages when deciding the "right way" to implement an activity because its emphasis on accommodating the multiple perspectives of the whole organization can result in a stronger acceptance level for compliance initiatives. This inclusiveness also can assist significantly when enlisting personnel to participate in the reporting, investigation, and corrective action processes.

Quality Improvement Initiatives

Of course, the cornerstone of any compliance program is its ability to assess the information it gathers, apply the assessed data to internal and external rules, and fix any gaps that are identified. When integrated into systems management concepts, this cornerstone correlates to quality improvement initiatives that seek to improve an organization's systems management. Several quality improvement initiatives including Total Quality Management (TQM), Malcolm Baldridge National Quality Award, and Six Sigma have found favor within healthcare circles. All of them have useful applications to compliance programs.

Total Quality Management. TQM is an organized set of management tools that facilitate the identification and repair of easy to solve problems. It works by enlisting people in a cross-disciplinary manner to help identify possible causes of recognized problems and then incorporating their observations and insights toward identifying the right solution. TQM gained favor due to its collegial, team-building approach. Also, TQM does not require a lot of data acquisition, management, or analysis, which has certainly contributed to its popularity. This attractiveness, however, is a key weakness. TQM operates from people's experience and intuition. The "right" solution is frequently the "popular" solution. This approach can be acceptable, but it often legitimizes entrenched behavior.

Malcolm Baldridge National Quality Award. The Malcolm Baldridge National Quality Award is given to businesses that are judged as outstanding in seven areas: (1) leadership; (2) strategic planning initiatives and capabilities; (3) focus on customers and markets; (4) knowledge and ability to measure and analyze data; (5) human resources capabilities; (6) process management capabilities; and (7) ability to achieve measurable results. The award assesses the end results, but does not recommend specific tools to use to achieve those results.

The seven Baldridge criteria are valuable in evaluating the effectiveness of a compliance program. The methodology is limited, however, in that it identifies only what an organization needs to achieve, or in other words, its quality improvement (QI) goals. It does not address, nor does it have any capability of supplying the tools to achieve those goals. Still, the Baldridge Award can be a useful QI tool for compliance initiatives because it offers a diverse framework for evaluating problems.

Six Sigma. "Six Sigma" is a statistical term, reflecting an ideal target of 3.4 or fewer defects per million processes. Because of its statistical underpinnings, the Six Sigma methodology focuses on gathering and evaluating hard data. Six Sigma does not rely on intuition, "common wisdom," or majority opinion, unlike some of the other quality improvement initiatives. This is more philosophically consistent with compliance activities for which rules must be evaluated from the concrete perspective of a healthcare organization's exposure and risk assessment. Concrete, action-oriented solutions need to become policy, to raise the healthcare organization to its desired level of safety – regardless of the difficulty or "grayness" of the law.

The Six Sigma management philosophy is perhaps the most popular quality improvement system in use today. It is certainly the most comprehensive, and is viewed by many of its often passionate devotees as a way of life rather than a mere QI tool.

Six Sigma is a process-improvement methodology based on concrete information. It is a structured, systematic approach utilized by businesses generally to improve the way they operate. What is and is not broken? If broken, how broken is it?

At its core, Six Sigma is a problem solving approach useful for any business system or for any business overall, tied to the ongoing reduction of "defects." This approach lends itself quite well to compliance initiatives, which also seek to identify what is or is not working within a healthcare organization and to minimize mistakes and other defects that affect compliance.

Six Sigma focuses on an organization's "processes." A process is any string of actions focused toward a particular goal or result. When a healthcare entity provides clinical services, submits accurate bills, reports potential problems or writes up incident reports, it is creating Six Sigma "processes." If an organization is dissatisfied with any of the end results of its processes, the dissatisfaction is evidence that a process is not functioning properly and needs to be modified. The next step under Six Sigma is to identify what aspect of the dysfunctional process has created the unsatisfactory result.

In the world of Six Sigma, the "correct" solutions to most defects must be identified from the perspective of the "customer," that is, the person or entity receiving (and presumably benefiting from) the end result of the Six Sigma process. How serious is a defect? This depends on how important the defective process is to the customer. How much time and money should you expend on fixing a defect? This depends on what the customer needs and values. The ultimate goal is to enhance the satisfaction of the "customer."

In the context of a compliance program, the definition of "customer" varies by activity. In training and monitoring activities, the "customer" is the healthcare organization's management team, which is relying on the quality of the learning process to shape understanding and implementation of compliance policies. In activities such as the evaluation of reimbursement accuracy and efficiency, or the evaluation of claims denials and appeals, the "customer" is the payer of the services, Medicare or otherwise. When evaluating marketing activities, joint ventures and so forth, the "customers" are the organization's senior management (who need the relationships to produce the benefits the healthcare organization seeks) as well as the co-venturing partners (who must be happy with the relationship) and, ironically, the compliance team itself (who must be able to attain an appropriate level of communication without inappropriately constraining these marketing activities).

Another aspect of Six Sigma that overlaps significantly with healthcare compliance activities is its focus on consistency. In the world of Six Sigma, varied results are a sign of a dysfunctional process and should be assessed carefully. As an example, if a hospital's medical director contracts with outside physicians, Six Sigma teaches us to impose consistent parameters among all of the contracts to ensure that haphazard customizing does not get in the way of obeying the pertinent federal laws that affect medical director agreements as well as the practical ease of monitoring such compliance. In addition, of course, haphazard customizing creates administrative difficulties, dangerous precedents, and the elimination of economies of scale.

Six Sigma favors a holistic approach to systems management. When embraced by an organization, Six Sigma permeates operations generally, affecting most everyone. This holistic approach suggests some rather interesting ideas for healthcare compliance programs. Even within healthcare organizations that use quality improvement tools, compliance initiatives are often viewed as a side operation. Sometimes this is because the organization doesn't quite know what to make of its compliance efforts. Sometimes this is because the organization mistakes the compliance program's need to be independent and beholden to no other department for a belief that the compliance activities, therefore, must work in relative isolation. But Six Sigma recognizes that most problems – compliance and otherwise – are caused by common defective processes, misunderstandings, vague allocations of responsibility, poor communications, etc. So, while a compliance program does need a substantial degree of autonomy and leverage to monitor and enforce its requirements effectively, its approach to problem solving and investigation necessarily cuts across all departments within the healthcare organization. Further, even when the compliance problem is resolved, the process defects identified can be fixed generally. A communication problem, when solved, usually will benefit operations generally, and not merely a specific compliance initiative.

These ideas barely scrape the surface of the many benefits systems management tools offer to compliance programs. There is substantial overlap between systems management concepts and healthcare compliance guidelines and opportunities and limitations to an integrated approach to compliance activities.

Neil Caesar is President of the Health Law Center (Neil B. Caesar Law Associates, PA), a national health law practice in Greenville, South Carolina, focusing on business opportunities and regulatory issues for healthcare providers. Mr. Caesar also is a principal with Caesar Cohen, Ltd. offering compliance training, outsourcing and consulting. A frequent author and speaker, Mr. Caesar is the author and editor-in-chief of the five volume Compliance Answer Book series and is a member of the CCH Health Care Compliance Editorial Advisory Board. Telephone: 864-676-9075, Email: info@healthlawcenter.com; website: www.healthlawcenter.com

Anti-kickback

OIG OKs cost-sharing assistance program

by Sheila Lynch-Afryl, J.D., Contributing Editor

A nonprofit, tax-exempt, charitable corporation's proposed program to provide assistance with premium and cost-sharing under Medicare Parts B, C, and D and Medigap would not constitute grounds for the imposition of civil money penalties, according to an Office of Inspector General (OIG) advisory opinion.

Premium support. The corporation's current programs for patients with specific chronic diseases include premium support, emergency relief, and nonfinancial assistance, such as assisting families with locating insurance. Under the proposed program, the corporation would expand its premium support program to offer financial assistance for premiums and cost-sharing obligations to financially needy Medicare beneficiaries under Part B, Part D, Medicare Supplementary Insurance, and Medicare Advantage.

Program funding. Most of the corporation's funding is provided by nonprofit organizations, home health agencies, manufacturers of drugs used to treat the diseases covered by its program, and suppliers that provide services to patients receiving assistance from the corporation. The proposed program will permit donors to provide unrestricted donations or designate that their funds be used either to support patients in a specific disease category or through a specific program, such as premium or cost-sharing assistance.

According to the OIG's advisory opinion, it appears unlikely that donor contributions to the corporation would influence any Medicare beneficiary's selection of a particular provider, practitioner, supplier, or product because the corporation is an independent organization that is not affiliated with any donor and the corporation awards assistance in a truly independent manner that severs any link between donors and beneficiaries. In addition, assistance will be provided based on a reasonable, uniform measure of financial need that will be applied in a consistent manner.

Similarly, the corporation's subsidy of premiums and cost-sharing obligations is not likely to improperly influence any beneficiary's selection of a particular provider, practitioner, supplier, or product because beneficiaries will be assisted on a first-come, first-serve basis, a determination of a patient's qualification will be based solely on financial need, and the subsidies will expand beneficiaries' freedom of choice. ■

OIG Advisory Opinion, No. 06-04, April 27, 2006, Health Care Compliance Reporter ¶500,139.

Medicare

Medicare re-enrollment requirements may deter fraud, CMS says

by Jay Nawrocki, M.A., Contributing Editor

All providers will be required to re-enroll with Medicare at a minimum every five years to verify the accuracy of enrollment information, according to a new *Final rule*, which becomes effective June 20, 2006. Providers will be required to update the information on their enrollment application, form CMS-855, or a variation thereof, anytime there is a change of the information on the form. In addition, CMS may require a provider to verify the information on its enrollment form at any time. CMS believes that requiring re-enrollment will be a strong deterrent in Medicare fraud and abuse.

Requirements. A provider will have 60 days upon receipt of notification to review the information in the last application on file with CMS to make any changes and certify by signature that the information is accurate, complete and truthful. Application forms must be signed by the practitioner, the sole proprietor, or an official who has the legal authority to enroll a corporation in the Medicare program and commit the organization to fully abide by the statutes, regulations and program instructions. This individual must have ownership or control interest in the corporation as well. Signature authority may be delegated to another individual when the information on the application is being updated voluntarily or changed by the provider. CMS will furnish a copy of the latest application form for the provider to review and is currently working on a system to complete this process electronically.

Fraud and abuse. CMS may conduct unannounced site-visits to verify that the information on the application is correct and that the provider has the equipment, staff and other necessary requirements to provide services to Medicare beneficiaries. These site visits will be conducted by a CMS contractor or fiscal intermediary. They will be separate from the site visits conducted by state survey agencies to verify conformance with the Medicare conditions of participation. In fiscal year 1998, CMS conducted site visits of suppliers of durable medical equipment, prosthetics, orthotics and supplies and denied 156 of 159 new applicants and revoked the application of 656 other suppliers out of the 2,091 visited. In many instances, CMS discovered no facility at the address listed on the application or an inactive telephone number.

During the sale of a facility, both the current owner and prospective new owner must submit an application. Failure of either to do so could result in denial of an application, a deactivation of a Medicare billing number, or sanctions and penalties. In addition, the *Final rule* specifically prohibits the sale or transfer of Medicare billing numbers or privileges by providers to any other entity.

Revocation and deactivation. An application will be revoked for providers that have not submitted a claim for a period of 12 months or longer. If a provider's application is revoked for one facility, all other applications the provider has submitted will be reviewed for accuracy of information. A provider must submit a new application when any application is revoked or denied. This will include a new survey, a new provider agreement, and a new billing number. An application will not be considered denied until all appeals are exhausted. In lieu of an appeal, a provider may submit a new application. An application can be deactivated; during a period of deactivation no claims will be paid. An application can be reactivated upon submittal of a new application. Reactivation does not require a new survey, provider agreement or billing number. ■

Final rule, 71 FR 9466, April 21, 2006, Health Care Compliance Reporter ¶700,007.

In the News

AHA approves prices transparency policy

The American Hospital Association's (AHA's) Board of Trustees announced a policy to make hospital prices more transparent. The AHA board wants the federal government to require states to expand their efforts to make hospital charge information available to consumers, including information about an enrollee's expected out-of-pocket costs prior to medical visits. It also wants federal-led research to clarify what type of pricing information consumers want and would use in their health care decision-making. In addition, the AHA wants a hospital-led effort to create consumer-friendly pricing "language" - common terms, definitions, and explanations to help consumers better understand the information provided. ■

AHA News Release, April 20, 2006.

OIG proposes exclusion of Alvarado

Following two mistrials in the government's attempts to prosecute Tenent Health Care, Alvarado Medical Center, and Alvarado Chief Executive Officer Barry Weinbaum for violating the anti-kickback statute, the Office of Inspector General (OIG) has announced its intent to exclude Alvarado from participation in federal health care programs. The OIG alleges that Alvarado entered into physician relocation agreements through which money was funneled to existing physician practices in exchange for patient referrals. Alvarado has 30 days to submit documentary and other evidence regarding whether the proposed exclusions are warranted. Alvarado would then have the right to an administrative appeal of the proposed exclusion.

OIG Press Release, May 8, 2006. ■