CCH Health Care Compliance LETTER

Volume 11, Issue 3 health.cch.com February 5, 2008

On The Front Lines 4

Third party relationships: Effectively managing risks by Alan Jedlicka, J.D., Contributing Editor

Trends 1

- Lawmakers will focus on MA plans, Medicaid oversight
- SEC official discusses obstacles to effective compliance programs

HIPAA 7

- HIPAA consultant pinpoints essential elements of a security compliance program

Fraud and Abuse 8

- DME company, infusion clinic owners sentenced for Medicare fraud

In the News 8

Lawmakers will focus on MA plans, Medicaid oversight

Lawmakers returning for the second session of the 110th Congress are expected to examine overpayments to Medicare Advantage (MA) plans, as well as MA plans' marketing practices, and oversight of the Medicaid program, according to House and Senate aides.

Senate Finance Committee Chairman Max Baucus (D-Mont.) intends to move bipartisan Medicare reform early in the year. The Finance Committee likely will tackle MA issues at one or more hearings in the first weeks of the session, said a Baucus aide. Baucus and House Ways and Means Health Subcommittee Chairman Pete Stark (D-Calif.) have expressed concerns about MA plan marketing abuses and overpayments to MA plans.

In 2006, Medicare payments to private health plans on behalf of enrollees averaged 112 percent of traditional fee-for-service costs for the counties where MA enrollees reside. Private fee-for-service plans—prevalent in rural areas where the benchmark rate is significantly higher than Medicare fee-for-service costs—are paid 119 percent of fee-for-service costs before adjusting for enrollee risk, according to a Henry J. Kaiser Family Foundation fact sheet.

The Medicare Payment Advisory Commission has recommended that the overpayments be eliminated. Stark said that savings from reduced MA overpayments could be used to offset the cost of halting physician payment cuts.

Stark also contended that not only do MA plans charge more for services ranging from home health care, hospital stays, and chemotherapy drugs to durable medical equipment, but agents also have been found to lie about MA premiums and physician participation in private plans to take advantage of individuals with serious language barriers or cognitive impairments and enroll beneficiaries who thought they were signing up for new Medigap plans in MA plans.

In addition to addressing possible Medicare reforms, the Finance Committee will exercise strong oversight of the Medicaid program to ensure that low-income Americans are getting the health care they need and deserve and that the program is operating effectively and efficiently, a Baucus aide said.

According to the aide, Baucus also plans to hold hearings to examine the best ideas for comprehensive health reform and to lay the groundwork for enacting legislation in the near future. "Effective health care reform will involve a mix of public and private solutions to get all Americans the quality health care they need, and Senator Baucus intends to lead an effort to find consensus on ideas that will really work—and can win sufficient support—to make sure that every American is able to get quality, affordable health care," the aide added. ■

CCH Washington Bureau, Jan. 23, 2008.

Wolters Kluwer Law & Business

SEC official discusses obstacles to effective compliance programs

The most common reason for compliance programs to fail or to be less than fully effective is that they do not operate within a larger culture of compliance in a firm, according to Lori Richards, Director of the Office of Compliance Inspections and Examinations at the Securities and Exchange Commission (SEC). Richards discussed five specific obstacles that compliance programs face in remarks prepared for a speech at the National Society of Compliance Professionals Membership Meeting in Washington, D.C., on October 18, 2007.

A culture of compliance is an overall environment that fosters ethical behavior and decision-making and instills in every employee an obligation to do what is right. Richards said that the culture of compliance must be part of the essential ethos of a firm so that when employees make decisions, whether large or small, and regardless of who is in the room when they make them, they are guided by a culture that reinforces doing what is right. Richards noted that a firm's cultural norms will be stronger than any new policy that a manager develops and talked about overcoming five major obstacles to achieve a strong culture of compliance.

Lack of management support. Richards characterized a lack of management support as the most destructive retardant to an effective compliance program. She gave the example of a newly registered investment adviser who asked a private lawyer for legal advice about a transaction. After the lawyer told the adviser that the transaction was clearly illegal, the adviser called the lawyer back and inquired as to what penalty the adviser would pay if he went forward with the transaction and was caught. The story stunned Richards because it so clearly showed a lack of any real management support for compliance.

Richards said that her Chief Compliance Officer (CCO) friends would say that this is a situation in which their placement within an organization might really make a difference. If the CCO has a seat at the table with other senior managers, the CCO might be able to bring his or her compliance perspective to bear and convince management that good compliance is good business.

CCOs provided the following suggestions for handling the situation:

- One CCO told Richards that he would work hard to make clear that he understands and supports the business and to find compliant solutions to problematic practices or proposals.
- Another CCO said that in this situation she might bring in an outside expert to educate senior management regarding their legal and fiduciary obligations and explain the serious legal, reputational, and business risks that exist in violating the law.
- A third CCO recommended finding a member of senior management who "gets it" and can champion the cause of compliance to his or her peers.

Risk-taking valued over all else. Noting that cultural values sometimes can clash, Richards observed that firms valuing risk-taking without limits will clash with a culture of compliance. She said that, in a firm that allows excessive deference to its big producer without really knowing how he or she gets the results, a CCO who tries to determine how the big producer gets the results may face pushback and even hostility.

To overcome this obstacle, Richards recommended education that emphasizes that compliance is not about stifling risk-taking or profit-making, but about helping to ensure that business is conducted within the firm's tolerance for risk. She advised that it may help to remind employees that the firm is bigger and more important than any one individual producer.

Employees who do not understand the value of compliance obligations. Richards observed that if a firm's employees do not affirmatively buy into the value and purpose of compliance, the compliance program will not be effective no matter how strong the CCO has developed the compliance structure. If employees don't understand what the CCO does or why he or she does it, they are a lot less likely to come to a CCO for advice when facing a vexing situation or to report possible problems.

Firms that grab their employees' attention with real world examples of

continued on page 3

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
Craig Arritola

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.

compliance issues through the use of videos and other techniques seem to have a better chance at getting employees to understand and value compliance efforts, according to Richards.

She stressed the importance of explaining the underlying reasons for the compliance policies and why they are good for the firm. Richards gave the example of a firm that was having a hard time getting its employees to comply with various anti-money laundering rules. When the CCO provided the employees with clear explanations about the purpose of these requirements and their role in possibly preventing terrorist financing, employees were much more willing to comply with the rules.

Richards praised employee training programs that are engaging and even entertaining while remaining focused on how compliance guidelines apply to employees in the specific context of their work. She also likes programs that are branded within the firm by using ad campaign-like tactics to get the word to employees that compliance is an easy resource to use.

Lack of resources. According to Richards, CCOs say the first step in ensuring that compliance efforts are adequately funded is to carefully determine if the firm needs additional compliance resources. If that is the case, the CCO should put together a clear and credible case for funding and be willing to take it up the chain of command. Richards suggested referring to regulators' expectations when making the case for adequate resources.

Richards said that her office at the SEC examines securities firms' compliance and supervisory programs for adequacy. If weaknesses are discovered, the examiners will probe most deeply into those areas for possible violations. The examiners determine the relative risk of each firm based on whether the firm has a healthy compliance program that is likely to identify and head off any compliance problems in the future.

Richards said that if violations exist and the firm is found to have an inadequate supervisory or compliance program, the SEC or another securities regulator may hold the firm responsible in an enforcement action.

Lack of constancy. The final obstacle to embedding a culture of compliance in a firm is lack of constancy, according to Richards. She said it is a common phenomenon for a firm to have a big compliance push, perhaps when new rules come out, but then employees may never hear about that issue again.

"A culture of compliance is an overall environment that fosters ethical behavior and decision-making and instills in every employee an obligation to do what is right."

A firm should not assume that it just needs to tell employees something once and they will know it forever. This does not work, said Richards, who stressed that repetition is the key to educating employees.

To ensure a culture of compliance, constancy is needed at all levels from the Chief Executive Officer down, according to Richards. She said the best examples of this occur in firms with senior leaders who often speak about the firm's culture and emphasize that doing what is right is what is expected of employees. These leaders repeat their message in many different ways, including written messages to the firm's employees, service providers, and shareholders. These leaders also make clear in meetings and in private conversations that the firm's decision-making process will be guided by this philosophy.

Richards suggested that to ensure constancy of message, a firm might inventory compliance obligations that rely on behavioral compliance and focus its ongoing message on those areas. She also recommended developing ways to get the message out in an interesting manner—again and again and again—as part of a long-term plan. ■

Susan Kavanagh has been the senior writer for the CCH Federal Ethics Report for the past 14 years.

Reprinted from the CCH Federal Ethics Report, Vol. 4, Issue 12, Dec. 2007.

Third party relationships: Effectively managing risks

by Alan Jedlicka, J.D., Contributing Editor

Third party agents typically are recognized as presenting certain legal risks that include exposure to the Foreign Corrupt Practices Act (FCPA) abroad and commercial bribery claims in the United States. Beyond the FCPA and commercial bribery, however, third party agents and representatives can expose a company to risks involving misuse of intellectual property, data security breaches, and more. Most companies maintain relationships with legions of third parties–consultants, sales representatives, distributors, staffing agencies, collection agencies, call centers, even joint venture partners and IT vendors–all of whom can expose a company to legal, compliance, and reputational risks. Effective compliance programs, therefore, need to include guidelines and procedures for managing the risks to which companies are exposed by their third party relationships. Global compliance leader, Eduardo Buso, discussed these issues in an address to the Society of Corporate Compliance and Ethics at its annual meeting held September 11–12, 2007, in New Orleans, Louisiana.

Consultants might present lavish gifts or entertainment to government officials, or misplace a laptop computer on which a company's customer information had been stored. Distributors could sell a company's goods to a sanctioned country. A staffing agency might provide workers to a company without first verifying immigration status, and a collection agency could be employing deceptive practices or intimidating a company's customers. To minimize exposure to such risks, a company's code of conduct—the starting point for most compliance programs—should set standards for company behavior that include third parties.

Code of conduct

According to Buso, a code of conduct establishing minimum standards for third party relationships would encompass certain distinct policy areas. An anti-bribery policy should authorize the use of third parties only for legal, legitimate business purposes. Privacy and data protection policies should be established to safeguard customer and employee information. Government contracting policies should require third party compliance with record keeping and other requirements, and international trade control policies similarly should require third party compliance with trade laws and regulations. Sourcing policies should eliminate illegal or high risk practices (for example, "sweatshops" or child labor), and intellectual property policies should make clear that third parties are required to protect a company's intellectual property and avoid improper use of non-company-owned intellectual property including software and licenses.

Risk assessment and mitigation strategies

The code of conduct, however, is only a starting point. To address third party risks, Buso stated that a compliance program also must include specific procedures and guidelines that apply to third party relationships presenting various degrees of risk. The risk assessment process will help to shape and refine mitigation strategies. The first step in the process involves getting the support of senior leadership. Risk assessment of third parties must be a high priority for the company. An inventory should be taken of all third parties used by the company. Every functional unit of the business must be engaged when compiling the inventory, which should group third parties by category. Next, rankings should be assigned to each third party according to degree of risk, whether low, medium, or high. Mitigation strategies should then be developed for each risk category, and third parties should be reviewed on a basis determined by risk level—higher risk requiring more frequent review.

Risk assessment factors concerning a third party sales representative, Buso said by way of example, might be based on the reputation the agent's territory or country has for corruption. A representative operating in a country that has a reputation

for very little corruption would have a low risk ranking; a country with some history of corruption, albeit non-pervasive, would have a medium risk ranking; and a country known to have a high level of corruption, a high risk ranking. A third party sales representative who has no interaction with the government or government agencies may be given a low risk ranking, while an agent who interacts with the government on sales, procurement, or other matters that involve decision making may have a high risk ranking. Mitigation strategies will vary according to a third party's risk ranking, but are fundamentally similar in that they all will include some degree of due diligence, written or contractual safeguards, training, and monitoring or auditing, Buso added.

Due diligence

Due diligence requires research and screening of each third party. Buso suggested conducting media checks, keying in to any adverse media, checking watch lists, or "blacklists," for any involvement with suspect activities or conduct, conducting government inquiries, performing reference checks, and even visiting a third party's office or work site. The higher the risk rating, the greater the due diligence, he cautioned. Concern over a third party's reputation, or an indication of prior misconduct, is sufficient cause to terminate relations with that particular agent. A contract cannot be drafted, Buso advised, around improper conduct. First-tier suppliers generally require enhanced or on-site diligence, although exceptions often can be made for large publicly traded suppliers that have good reputations with respect to compliance matters. Sub-tier suppliers, especially those that purchase a large percentage of their products from one particular company, should be subjected to greater diligence.

"To address third party risks … a compliance program … must include specific procedures and guidelines for risk assessment that apply to third party relationships presenting various degrees of risk. The risk assessment process will help to shape and refine mitigation strategies."

The scope of due diligence in risk assessment should include environmental conditions, wage and hour laws, forced or child labor, and working conditions, Buso noted. Operational plans and procedures, and plans for emergencies or accidents, also should be reviewed for compliance with applicable laws and standards. Third parties must not use prison labor, involuntary labor, or forced labor of any kind. Screening and documentation must eliminate any possibility of child labor and foreign contract workers working against their own will. Working conditions must include safe and healthy environments, clean, well lit and ventilated facilities, emergency exits and procedures, potable water, sanitary facilities, and fire safety equipment and alarms, Buso stressed.

Written or contractual safeguards

Written or contractual safeguards also depend on the third party's risk ranking and should include, at a level commensurate with the risk, the terms of compensation and reimbursement, written notice of all legal and compliance obligations, a written agreement that incorporates the company's code of conduct, and all compliance obligations specific to the agent. For high risk third parties, Buso advised that provisions be included for termination upon breach, as well as auditing or monitoring rights.

Training

Training requires, at a minimum according to Buso, providing a third party with a copy of the company's code of conduct. As the level of risk increases, the third party may be required to provide acknowledgement that the code of conduct was received and understood. Depending on the nature of the third party relationship, it may also be necessary for the third party to provide training on compliance obligations for its own employees, or to provide an acknowledgement that its employees were trained on compliance obligations.

Third party monitoring and audit procedures

Third party monitoring and audit procedures must reflect the nature and degree of risks presented by the agent. Lower risk may only require occasional watch list, or blacklist, checks, and renewed media searches. As the level of risk increases, so should the frequency of watch list and regulatory database checks. Training may be reviewed annually, and for high risk levels, annual office or work site visits and audits may be required. Close monitoring of a third party's activities and requiring agents to submit audits of their activities might be appropriate for higher risk rankings, but Buso advised checking with a legal department first.

Written guidelines, documented procedures

Documentation is the cornerstone of risk mitigation efforts, according to Buso. Business managers must be able to specify a legitimate need for a third party representative. Typical business justifications include customer access, industry knowledge, and the ability to cover a particular territory. Buso even suggested that business managers should be required to docu-

ment the justification for the third party representative and take ownership of that relationship from "cradle to grave."

Once a business necessity has been shown, procedures for working with third party representatives require a review of local laws. It must be determined in advance of any third party relationship whether local laws require a local legal representative, or whether third party representatives are permitted for government sales. It is also a key advantage, Buso pointed out, for a company to know of any local laws that might limit a company's ability to terminate third party sales representatives.

Third party qualifications

Following a review of the local law, Buso continued, an agent's qualifications must be reviewed. Financial resources are a significant factor, as are industry knowledge and experience. The experience and qualification of a third party's employees should be considered as well, especially when those particular employees will be working directly for the company. Third party representatives should be required to make detailed applications, which would include full disclosure of officers, principal shareholders, and government relationships.

Such application and disclosure facilitates effective due diligence. Detailed checklists should be included in the guidelines and procedures for conducting due diligence of the third party's company, officers, primary shareholders, and key employees. Outside investigative resources may be used as appropriate, Buso added, provided the firms are reputable and detailed letters of engagement are retained by the company. Thorough reference checks must be required and documented.

Discussion of code of conduct

Procedures should require a discussion of the company's code of conduct with the third party, which also must be documented. Buso recommended discussing the code of conduct in face-to-face meetings that include legal and compliance representatives. Matters that should be addressed in the meetings include the local business climate and business practices, the third party's understanding of and willingness to comply with the company's code of conduct, whether the third party has a code of its own, and any experiences the third party has had working with other companies.

The guidelines and procedures require senior executive approval, and completion of the procedures should be reviewed by company legal counsel, Buso noted. The procedures should require a written agreement indicating compliance with all applicable laws, compliance with the company's code of conduct, should the code of conduct exceed the applicable laws in terms of their respective levels of "robustness," the right to unilaterally terminate the relationship for breach, and provisions for renewal.

Conclusion

The key to successful efforts aimed at mitigating legal and compliance risks presented by third parties, Buso concluded, is that all third parties must understand and "buy in" to the compliance culture. Accountability is another key factor—accountability of the third party representatives for the risks they present, as well as accountability of the business managers for the third party representatives they recommend. Buso emphasized that a third party must never be engaged for something the company itself would not do, and companies must move quickly in response to any compliance concerns involving a third party. ■

Alan Jedlicka, J.D., is an associate writer/analyst at CCH, Inc., and the editor of the CCH Consumer Product Safety Guide. He also is a contributing writer for the CCH Federal Ethics Report, covering topics of corporate ethics and compliance.

Reprinted from the CCH Federal Ethics Report, Vol. 15, Issue 1, Jan 2008 .

HIPAA consultant pinpoints essential elements of a security compliance program

If you haven't taken at least the following seven steps toward compliance with the HIPAA security rule, you'll be hard pressed to convince someone that you're in compliance, according to Tom Walsh, president of Tom Walsh Consulting, LLC, in Overland Park, Kansas. Walsh conducts security training, risk analysis, and remediation activities for health care clients. Speaking at a January 17, 2008, American Health Information Management Association (AHIMA) audio conference, Walsh stated that organizations must: (1) appoint an official to oversee the security compliance program; (2) set standards of expected conduct; (3) train and educate staff; (4) develop a process for receiving reports of violations; (5) develop a process for responding to the reports; (6) audit and monitor compliance; and (7) take appropriate corrective actions when there is a violation.

Security compliance official. Organizations must assign someone with responsibility for overseeing information security. Walsh suggested appointment of a privacy and security officer that reports to someone high up in the organization. "Provide high visibility for the information security officer [(ISO)] position. Distribute an executive memo to the entire workforce formally announcing the appointment of the ISO [and] include the ISO's name and contact information," he recommended. "The main thing is that everybody should know who it is." He added, "If the memo comes from the [Chief Executive Officer], it adds more credibility."

Standards of conduct. Next, Walsh said, the organization should set standards of expected conduct and memorialize them in written policies and procedures, guidelines, or standards so people know what the expected behavior is. The information should be visible. "Make sure that people can find it. Too often we shove everything out on a network drive," Walsh said. The information should be easy to read and targeted to both the general workforce and information technology (IT) employees, he said, noting that the policies often are written by an information security professional for an information security professional. "We've got to make them simple to read and understand," he stressed.

Health information management (HIM) professionals can help write policies and procedures. "That's one area where I think [they] could really contribute," he said. Angel Dinh, a manager of professional practice resource at AHIMA, recommended that all staff contribute to security. "If you are not contributing, I would recommend that you do. Security is really an area where HIM and IT meet and expertise in both is needed to make compliance successful," she said.

Training and education. Training needs to include all staff, Dinh noted. Walsh pointed out that many managers with whom he has spoken believed they were exempt from training requirements. "They're probably the ones who need the most training," he said, noting that management has to make many of the decisions regarding risk. Walsh suggested establishing a formal information security training program that documents audiences, content, and delivery methods (*e.g.*, syllabus, attendance sheets, handouts, etc.). The program should include detailed security training for specific audiences and periodic security awareness for everyone, he said.

Incident reporting. Organizations should have a process for reporting and tracking incidents and emphasize that incident reporting is there to correct current incidents and avoid future ones, not to punish employees. "Our goal is to take corrective measures," Walsh stressed. It is important to measure the cost of the incidents, which can help justify the cost of establishing a different security control. Business associates also should know when to report incidents, how to report them, and to whom to report them. Walsh has found that most business associate agreements do not include this information.

Incident response procedures. Entities should create an incident response team and develop a plan for responding to incident reports. "You want to think about this well in advance. Have a plan for how to address it," Walsh said. He emphasized the importance of making those decisions before a crisis has occurred and noted his observation that most health care organizations lack incident response procedures. "You have to be very cautious when there is an incident," he added.

Incident response team members and other IT staff should be trained on collecting and handling evidence during an investigation, and the organization should establish remediation or action plans to prevent similar incidents in the future, he advised.

Auditing and monitoring. The next step, according to Walsh, is to conduct ongoing auditing and monitoring for compliance. Security officers should determine user activities and events that trigger an audit log entry, implement procedures to periodically review compliance, establish an audit log retention schedule, and establish an evaluation and validation process.

Corrective actions. When taking corrective actions (*e.g.*, sanctions, risk management, security controls, etc.), officers and management should make sure that sanctions are applied consistently. "Within our workforce, we'd better be consistent in how we enforce things," Walsh stated. Enforcement should focus on containing and taking appropriate actions. Walsh also recommended reducing risk to an acceptable level, which could require beefing up administrative, physical, and technical security safeguards and controls.

Compliance should not be the only driver for security, Walsh concluded. "We should be doing security because it makes good business sense, not because the government is telling us to do it." Documentation and demonstrated practices along with management support are the best indicators of a real information security program, he added. "It's got to have all of those elements together to make it work." ■

CCH Washington Bureau, Jan. 23, 2008.

Fraud and Abuse

DME company, infusion clinic owners sentenced for Medicare fraud

Nine owners of Florida-based health care companies have been sentenced to prison terms within the past several weeks for filing fraudulent claims for Medicare payment for a collective $59,599,832 worth of unnecessary durable medical equipment (DME) and infusion therapy, according to the U.S. Department of Justice (DOJ). The cases were brought through the efforts of the Medicare Fraud Strike Force, a multi-agency team of federal, state, and local investigators that was designed specifically to combat Medicare fraud in South Florida.

The nine individuals included several owners of fraudulent DME companies that had nothing to do with providing health care or necessary medical equipment. The companies submitted claims to Medicare for unnecessary medical equipment, such as oxygen concentrators, hospital beds, pressure reducing mattresses, orthotics, wound therapy pumps, expensive wound care items, prosthetics, and ostomy supplies; and caused the submission of false claims for pharmaceuticals. Also among those sentenced was the owner of a fraudulent HIV infusion clinic that billed for unnecessary procedures such as paravertebral joint injections.

The sentences imposed on these individuals ranged from 19 to 87 months in prison. Assistant Attorney General Alice Fisher of the DOJ Criminal Division said, "The [DOJ] places a high priority on investigating and prosecuting those who steal tax payer money intended to provide health care for the elderly and disabled." She added, "We have dedicated a team of experienced prosecutors to focus on Medicare and other health care fraud around the country."

Alexander Acosta, U.S. Attorney for the Southern District of Florida, emphasized, "The fight against health care fraud in Miami is a top priority. With the help of the newly formed [HHS Office of Inspector General] Florida region, which will add federal agents to our efforts, we expect to see a significant impact on reducing fraud." ■

DOJ Press Release, Jan. 23, 2008.

In the News

U.S. joins FCA cases against three New Jersey hospitals

The United States has intervened against three New Jersey hospitals in two *qui tam* suits alleging that the hospitals defrauded Medicare, the Department of Justice (DOJ) announced. Both *qui tam* suits alleged that the three hospitals fraudulently inflated their charges to Medicare patients to obtain enhanced reimbursement from Medicare. In addition to its standard payment system, Medicare provides supplemental reimbursement, called "outlier payments" to hospitals and other health care providers in cases in which the cost of care is unusually high. The supplemental outlier payments were enacted to provide hospitals with an incentive to treat inpatients whose care requires unusually high costs. Three individuals filed lawsuits against the three hospitals in 2002 under the whistleblower provisions of the False Claims Act.

DOJ Press Release, Jan. 24, 2008.

Former hospital executives' convictions overturned

A federal appeals court overturned the convictions of two former hospital executives accused of paying a state senator to advance the hospital's financial interests. The government alleged that the executives offered the senator a disguised bribe in the form of a sham job at one of the hospital's subsidiaries in exchange for the senator: (1) promoting the hospital's interests with respect to pending legislative matters; (2) lobbying several municipal officials to increase the number of patients brought to the hospital by ambulance service; and (3) facilitating meetings at his government office between one of the executives and representatives of two major insurance companies to resolve longstanding disputes about reimbursements owed to the hospital. The appellate court found that the executives' conduct with respect to the insurers, as well as the senator's actions in blocking or promoting legislation to favor the hospital, were properly considered as potentially criminal. The instructions given to the jury, however, were overly broad insofar as they allowed the jury to consider the ambulance service advocacy as a deprivation of honest services owed to the public.

United States v. Urciuoli; United States v. Driscoll, 1st Cir., Nos. 07-1297, 07-1327, Jan. 18, 2008.

Physician-owned hospitals need more oversight

CMS should develop a system to identify and track physician-owned specialty hospitals, ensure that a nurse is on staff 24 hours a day, seven days a week, and ensure that such hospitals have emergency response measures in place, according to recommendations in an Office of Inspector General (OIG) report. According to the OIG's evaluation of physician-owned specialty hospitals' ability to handle medical emergencies, half of the hospitals had emergency departments, but they generally had only one bed set aside for emergency purposes. Of the eight sample days reviewed, seven percent of the hospitals did not have a nurse on duty or a physician on call 24 hours a day, seven days a week. The lack of adequate staffing was most likely to occur during the weekends. Less than one-third of the hospitals had a physician on site at all times, and two-thirds of the hospitals relied on calling 9–1–1 as a part of their emergency protocol. The OIG also found that many of the hospitals did not have emergency procedures outlined in their written management policies. In response to the OIG report, CMS is examining these hospitals through routine surveys, has issued a memorandum to state agencies regarding emergency requirements for these hospitals, and will examine whether any regulatory changes are required to deal with equipment and staff issues for these hospitals.

OIG Report, No. OEI-02-06-00310, Jan. 11, 2008, Health Care Compliance Reporter ¶530,650.