CCH Health Care Compliance LETTER

Volume 10, Issue 8 health.cch.com April 17, 2007

IRS comments on tax-exempt executive compensation

by Torie Cole and George Jones, Contributing Editors

Heightened scrutiny by the IRS has brought the issue of executive compensation to the forefront of corporate governance in the nonprofit sector, according to Nancy Kuhn and Susan Cobb, Counsel for Powell Goldstein, LLP, Washington, D.C. Kuhn and Cobb sat down with CCH on March 12 to discuss the excess executive compensation initiative, conducted by the Exempt Organizations Office of the IRS's Tax Exempt and Government Entities Division (TE/GE), from a tax practitioner's perspective. Both practitioners provided their reflections on the latest TE/GE Report on Exempt Organization Executive Compensation Compliance Project and expectations on how it will impact their practice.

Kuhn noted that the results of the TE/GE report illustrate how the IRS is not particularly opposed to high salaries in general; only "unreasonable compensation." Executives working in the nonprofit sector are not expected under the law to work for less than their for-profit counterparts, and the IRS is not attempting to determine reasonableness purely based on a high salary level. Nevertheless, Kuhn acknowledged that there is a definite political aspect to the debate, with Senator Charles Grassley, Senate Finance Committee ranking member, recently leading the charge in remarking that "the IRS study and the recent revelations of the champagne lifestyles of certain nonprofit executives make it clear that the IRS needs to send clear signals of what's acceptable for disclosure and compensation at our nation's charities."

Kuhn and Cobb added that they have noticed in their practice that the issue of high compensation also has begun to attract the attention of regulators, both on the federal and state levels. "There is a lot more audit activity by the IRS in this area than two years ago," according to Kuhn. She estimated that this increase is magnified by media reports on the issue, capturing the attention of Congressional leaders, who in turn place pressure upon the IRS to improve compliance in this area. Kuhn noted that Senator Grassley has requested a report from the IRS by April 1, 2007, on the top 20 issues of noncompliance in the areas of public charities and private foundations. Cobb added that executive compensation compliance issues have also attracted examinations from State Attorney Generals who are concerned with the fiduciary responsibility of insiders of tax-exempt organizations.

The IRS's allowance of high but not excessive executive salaries, coupled with close public scrutiny, seems to have resulted in a general increase in the need for tax practitioners in the charitable sector. According to Cobb, the area is also growing as a result of the rules becoming more complex and the steeply rising penalties and

continued on page 2

Wolters Kluwer Law & Business

excise taxes. She pointed out that intellectual property issues and joint venture arrangements, which are fairly routine for taxable entities, require extensive planning and sophistication in the realm of tax-exempt entities.

Internal controls. While the Sarbanes-Oxley Act of 2002 (SOX) does not explicitly regulate the charitable sector, Cobb and Kuhn suggest that the executive compensation initiative should persuade practitioners in the exempt area to acquaint themselves with the increasing reach of SOX. The prohibitions on excess executive compensation and loans to disqualified persons under the *Pension Protection Act of 2006 (PPA)* are strikingly similar to the required internal controls under SOX. And, while SOX does not apply to public charities, Cobb pointed out that the socially conscientious and active board members of these entities often attempt to comply with the law anyway. "Even some small charities ask us whether they should have an audit committee," she notes. She also disclosed that the IRS has been circulating unofficial draft guidance on corporate governance for tax-exempt entities. ■

CCH Washington Bureau, March 15, 2007.

Medicare

PRRB focuses on reducing case backlog

by Paul T. Clark, Contributing Editor

Even though the role of the Provider Reimbursement Review Board (PRRB) is in flux, the PRRB is diligently working through a large backlog of cases and seeking to improve the process by which intermediary decisions are appealed. Speaking at the American Health Lawyer's Association conference on Medicare and Medicaid in Baltimore on March 22, PRRB chairman Suzanne Cochran noted that the PRRB is working through a backlog of 6,000 cases and offered guidance for attorneys working with providers who have requested PRRB hearings.

Cochran noted that the PRRB's role is in flux for two reasons. One is that CMS has to decide by this summer whether to issue a final rule regarding changes in the PRRB process. CMS issued a proposed rule on PRRB changes in June 2004, and by statute the agency within three years either has to issue a final rule or re-issue the proposed rule. At the same time, CMS is currently processing bids for the new Medicare Administrator Contractors (MACs) that are replacing the current system of intermediaries and carriers. Cochran pointed out that based on the request for proposals she has seen so far from possible MAC contractors, the new MACs are indicating that they expect to be involved in substantially fewer hearings with the PRRB compared with the existing level of cases involving intermediaries.

Tips for attorneys. Cochran said that the PRRB is resolving its backlog of cases at the rate of about 2,000 per year. She added that PRRB is taking particular notice of old cases, some of which have cost reporting years ending as long ago as 1994 and 1995. Many of these old cases involved group decisions.

Cochran also requested that attorneys take more care with the position papers they file in advance of a hearing with the PRRB. She said that in some cases the initial position paper was worded so vaguely it was difficult to figure out what was at issue. Then, this initial paper often would be replaced only days before a hearing with a position paper highlighting a different set of issues. According to Cochran, the PRRB is sending out several letters to providers involved in older cases asking that they submit final position papers as soon as possible, with the underlying data sent along to the intermediaries, and not wait until the hearing date is only days away. She said that the PRRB's plan is "not to impose penalties but to provide disincentives to let cases drag on."

Cochran warned that in the future, the PRRB will be much less likely to agree to multiple continuances for a case, and will be less likely to accept as an excuse for a continuance that the provider has recently changed its legal representative.

Best practices. Cochran outlined some of the best practices for attorneys waiting for PRRB hearings:

- Let the PRRB know as soon as the date for hearing is set if the date will not work; don't wait until days before the hearing to request a rescheduling.

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.
Stacey Fahrner, J.D., M.P.H.
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.

- When requesting a hearing, let the PRRB know if there are other cases with the same representative and the same issues pending, so the PRRB can decide if cases should be consolidated.
- Although the PRRB does not have the authority to subpoena the intermediary or request that it file papers in the same timely manner as the provider, provider representatives can request as part of the position paper that the intermediary meet specific deadlines for filing its supporting evidence.

Cochran says she has no idea what will happen to the backlog of cases as intermediaries are replaced by MACs and stressed the problems inherent in cases that might cross over to multiple MAC jurisdictions. She reminded her audience that Congress established the PRRB as an entity independent of CMS as a resource to help federal courts figure out the issues underlying individual cases. Cochran emphasized, however, that the PRRB has no communication with CMS as to what its role will be under the new MAC system. ■

CCH Chicago Bureau, March 22, 2007.

CAP final rule includes protections for physicians, beneficiaries

by Valerie L. Witmer, J.D., Contributing Editor

Nearly one year after submitting a proposed rule for public comment, CMS has issued a final rule to phase in the competitive acquisition program (CAP) for durable medical equipment, prosthetics, orthotics, and supplies (DMEPOS) under Medicare Part B. The CAP, which is required by the Medicare Prescription Drug, Improvement & Modernization Act of 2003 (MMA) (PubLNo 108-173) § 302(b), will be phased in over several years and will replace the current DMEPOS fee schedule payment amounts for certain items with payment rates derived from the competitive bidding process.

Response to public comments. In response to comments on the proposed rule, CMS has added new protections for physicians and other health care professionals, as well as small suppliers. The final rule includes a limited exception to the competitive bidding requirement that will allow physicians, physician assistants, clinical nurse specialists, nurse practitioners, and private practice occupational and physical therapists to provide certain competitively bid items to their own patients as part of their professional services without having to participate in the bidding process. Additionally, the rule allows a physician or other treating professional to prescribe a specific item, brand, or mode of delivery when necessary to avoid an adverse medical outcome, and requires the supplier who has been awarded a contract by CMS to furnish items under the CAP ("contract supplier") to make a reasonable effort to furnish the product or mode of delivery as prescribed, find a suitable alternative product, or find another contract supplier in the competitive bidding area (CBA) who can provide the product.

CMS has included in the final rule several provisions that will ensure small supplier participation and access to the competitive bidding market. The rule provides for a 30 percent target number for small supplier participation and establishes a methodology to achieve that goal. It also allows small suppliers that cannot service the entire CBA independently to form networks in order to participate in the bidding process. Additionally, small suppliers will not be required to submit bids for all product categories, but rather will have flexibility to choose the product categories on which they will submit bids.

The final rule also adopts some special protections for beneficiaries in the CBAs who are already renting certain DMEPOS items when the CAP becomes effective, including a grandfathering provision that may enable these beneficiaries to continue renting items from their existing suppliers, rather than having to switch to a contract supplier. Further, beneficiaries who own an item of DMEPOS that is on the competitive bidding list will be allowed to receive maintenance and servicing from any Medicare supplier, and

continued on page 7

On The Front Lines

Handling HIPAA complaints and security incidents

by Jonathan P. Tomes, Esq., Contributing Editor

With enforcement of the Health Insurance Portability and Accountability Act (HIPAA) starting to pick up-four criminal convictions and more than 20,000 complaints to the Department of Health and Human Services (HHS)-properly handling complaints and security breaches is crucial to avoid criminal and civil liability, adverse publicity, HHS investigations, and angry patients. This article discusses the proper handling of complaints and security incidents under the HIPAA requirements.

Complaints

A number of HIPAA rules require covered entities to properly handle complaints about the misuse of protected health information (PHI) and security breaches.

First, 45 C.F.R § 160.306 allows an individual to file a complaint with the Secretary of HHS through the Office of Civil Rights if the individual believes a covered entity has violated the HIPAA privacy or security rules. Section 160.306 further specifies that the complaint must:

- be filed in writing, either on paper or electronically;
- name the entity that is the subject of the complaint and describe the conduct believed to be a HIPAA violation; and
- be filed within 180 days from the time the complainant knew or should have known of the violation, unless this time limit is waived by the Secretary for good cause shown.

The Secretary may investigate complaints filed under § 160.306. Such investigation may include a review of the pertinent policies, procedures, or practices of the covered entity, as well as a review of the circumstances surrounding any alleged acts or omissions implicating compliance with the privacy or security rules.

To date, most HIPAA complaints have not turned out to be valid; yet HIPAA compliance will be complaint driven. In other words, covered entities do not have to worry about periodic or random audits by HHS, just investigations in response to complaints. These investigations are undesirable because, even if the organization has not violated HIPAA, responding to such investigations is a hassle. Moreover, a valid complaint could result in a referral to the Department of Justice for criminal prosecution or an administrative fine pursuant to 45 C.F.R. subpart E.

Second, if the organization has a good internal complaint system and, perhaps, a little luck, the individual may complain to someone within the organization rather than to HHS, often enabling the organization to resolve the matter internally and avoid an HHS investigation altogether.

The Privacy Rule, 45 C.F.R. §164.530, requires certain personnel designations as part of an organization's internal complaint system. Specifically, a covered entity must designate a privacy official who is responsible for the development and implementation of the entity's policies and procedures. In addition, the entity must designate a contact person or office who is responsible for receiving complaints and able to provide further information about matters covered by the notice of privacy practices.

The Privacy Rule also requires that a covered entity have a complaint process as well as a process for documenting complaints:

- a covered entity must provide a process for individuals to make complaints concerning the covered entity's HIPAA policies and procedures or its compliance with such policies and procedures or the requirements of HIPAA; and
- a covered entity must document all complaints received, and their disposition, if any.

Under § 164.520(b)(i)(vi), the entity's Notice of Privacy Practices must inform individuals upon whom it maintains PHI how to complain and must include:

- a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated;
- a brief description of how the individual may file a complaint with the covered entity; and
- a statement that the individual will not be retaliated against for filing a complaint.

In addition, the Notice of Privacy Practices must contain a description of how the individual may complain to the covered entity or to the Secretary of HHS. The description must include the name, or title, and telephone number of the contact person or office responsible for receiving complaints.

Likewise, under 45 C.F.R. § 164.520(b)(vi), if a covered entity denies a person access to or amendment of PHI under § 164.526, the denial must contain a description of how the individual may complain to the covered entity pursuant to the

complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated to receive such complaints.

Covered entities may not take adverse action against a complainant. Under § 164.530(g), a covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for: (1) exercising his or her rights under HIPAA, including filing a complaint under § 164.530; (2) filing a complaint with the Secretary under § 160.306; (3) testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under 45 C.F.R. part 160; or (4) opposing any act or practice made unlawful by HIPAA, provided (a) the individual has a good faith belief that the practice is unlawful, and (b) the manner of the opposition is reasonable and does not involve an improper disclosure of PHI.

Third, the Security Rule requires response and reporting procedures for identifying and responding to suspected or known security incidents, mitigating harmful effects of security incidents, and documenting such incidents and their outcomes. (See 45 C.F.R. § 164.306(5)(ii)).

Types of complaints. Generally, two types of complaints are possible. The first type includes complaints by individual patients, clients, family members, or personal representatives, and typically will involve perceived violations of their HIPAA rights. These complaints likely will result from notifying individuals of their rights pursuant to the entity's Notice of Privacy Practices.

The other type includes complaints by employees or others who maintain, use, or transmit PHI. These complaints typically will involve reporting problems that may endanger individual privacy or the covered entity and should come from the entity's response and reporting policies that are part of its security incident procedures.

Who should receive complaints? With respect to complaints by individuals, the complaint official requirement under § 164.530(d), above, does not provide any guidance on the qualifications of such an official. The complaint official could be any one of the following:

- privacy officer;
- ombudsman;
- patient/client representative; or
- other qualified individual.

In selecting a complaint official, keeping some insulation between the person who receives the complaint and the person who acts upon it normally will be wise. The complaint officer, rather than the chief executive officer or the only clinician in a small practice, should tell the patient that the covered entity has thoroughly investigated the complaint and found it to be invalid.

Security incidents

Again, HIPAA provides no specific guidance as to how security incident procedures are to be accomplished. Covered entities should have a formal procedure to handle such incidents, including a report procedure, a response procedure, and procedures to mitigate the harmful effects of security incidents.

Reporting security incidents. A covered entity's reporting procedure could require members of the entity's workforce to report security incidents to the same complaint official established for receiving individuals' complaints under § 164.530(d). A better choice might be to have them report to the security officer, which is required under § 164.308(a)(2). In small operations, however, one individual may be all three—privacy officer, security officer, and complaint official.

To comply with the security incident procedure requirements, a covered entity must have a formal reporting and response procedure. Reporting procedures are not difficult to draft. They should specify what must be reported, to whom an employee or other person must report a security breach, the form of the report, and that the employee must make such a report as soon as he or she detects the breach. A key point here is that workforce members must report not only actual breaches of security or confidentiality but also breaches of the organization's policies, procedures, and security measures protecting PHI, whether or not such a breach actually results in any compromise of that PHI.

For example, if the organization's policy requires certain employees to log off when they leave their workstation, and one employee does not, that most likely is a breach of the workstation use policy that should be reported even if the employee's supervisor discovered it 60 seconds later and no unauthorized person viewed any data on the screen. Such a minor breach ordinarily would not result in a major response; but if the employee in question continuously forgets to log off, the next time, the damage might be catastrophic.

Responding to security incident reports. Response procedures specify what happens after responsible individuals receive a report of a security breach, including whom the response official must notify, who investigates, who gets the report of investigation, who takes remedial action, and ho takes disciplinary action.

Because of the speed at which one can create, alter, destroy, or steal data, rapid response is mandatory. As to immediate action, two basic approaches should be considered: (1) the "protect and proceed" approach and (2) the "pursue and prosecute" approach.

The primary goal of the protect and proceed approach is the protection and preservation of the system and its data. The facility tries to actively interfere with the intruder's processes, prevent further access or security breaches, and immediately begin damage assessment and recovery. This ap-

proach may involve such actions as shutting down the system, closing off access to the network, et cetera, and has at least a couple of drawbacks. For example, the facility may not be able to identify the breaching party, and the system may be down during peak use.

The other approach, the pursue and prosecute approach, is intended to allow those people who are breaching security to continue to do so until the organization can identify them. This approach is better for disciplining those responsible for the breach, but has the big drawback of increasing potential liability for damage or alteration to the system or its data, or loss of confidential information.

Considering the critical nature of medical information and the potential liability for its loss, alteration, or breach, the protect and proceed strategy normally will be preferable for a health care organization.

After taking immediate action, the responsible person should:

- conduct an investigation;
- take necessary disciplinary action; and
- take necessary corrective action.

A thorough investigation is critical to determine how and why the breach occurred. Larger organizations should consider selecting a response team for major incidents, which should include personnel from legal or risk management, computer security, overall security, technical (computer department), health information management, and human resources. The investigator(s) should:

- collect all records and documents and preserve all relevant data in files, systems, or individuals' possession;
- interrogate employees and others involved;
- draft memos to preserve findings in writing and brief management; and
- take disciplinary action, if appropriate.

Section 164.308(a)(2) of the Security Rule requires covered entities to have a sanction procedure "against workforce members who fail to comply with the security policies and procedures." The sanction policy should be a system of progressive discipline from verbal warning to termination and possible referral to law enforcement or professional licensure agencies or other authorities. If a good employee forgets to log off and the breach is caught before any harm is done, a verbal warning probably will be appropriate. If a transcriptionist discusses a patient's genital herpes at a party, termination would be appropriate–if not mandatory–based on the seriousness of the offense, even if the transcriptionist is the best transcriptionist in the history of medicine.

Some covered entities tend to overreact to HIPAA violations with a knee-jerk "Oh no! HIPAA violation! Fire them!" Although organizations certainly should take HIPAA violations seriously, firing everyone who commits a minor breach may not be realistic if, for example, an organization's entire medical staff accesses the chart of a celebrity patient improperly, i.e., without any bona fide medical or business need to do so.

Mitigating the harm of security incidents. Both the Security Rule and the Privacy Rule impose on organizations a duty to mitigate the potentially harmful effects of security incidents. (45 C.F.R. § 164.308(6)(ii); 45 C.F.R. § 164.530). Mitigation has two aspects—ensuring that the breach does not happen again and lessening the harm caused by the breach.

Such things as recovering the data that was the subject of the breach or warning the improper recipient not to redisclose it could lessen the harm. If the breach could result in identity theft, the covered entity might mitigate the potential harm by notifying law enforcement and the patient whose PHI was the subject of the breach so they could take steps to protect themselves from identify theft. The Veterans Administration complied with this part of HIPAA when it sent letters to all of the veterans whose PHI might have been on missing laptops, warning them of the possibility of identity theft and advising them of what they could do to protect themselves.

HIPAA does not require covered entities to notify a patient of a privacy or security breach unless the patient requests an accounting under 45 C.F.R. § 164.528. This seeming lapse in the regulations exists because notifying the individual could result in more harm than the breach itself—especially if the breach was both minor and quickly contained. For example, notifying a mental health client being treated for paranoid ideations that his clinician has breached confidentiality could ruin the therapeutic relationship and put the client in more danger than could ever result from the minor, quickly contained breach. Thus, the covered entity must determine whether notifying the individual is necessary to properly mitigate the potential harm of the breach, such as by alerting the individual to the possibility of identity theft.

To prevent this type of breach from recurring, the covered entity should review its security measures, policies, and procedures to determine whether any corrective action is necessary. Corrective action could include: (1) disciplinary action, if the breach was caused by failure to follow policies and procedures; (2) more training tailored to the problem area that caused the breach; and (3) revising policies and procedures.

The Security Rule's response and report requirement requires covered entities to keep records of any security incident, including the outcome of the response and report procedure, for six years.

Using the full response and report procedure may not be necessary for complaints by individuals. In other words, a formal investigation may not be necessary, but the organization still must verify the facts. The organization's response and report policy should specify when the matter is to be referred for formal investigation. An individual's complaint that the Director of Health Information Management would not give the individual a copy of his or her medical records would not involve a security incident, and therefore would not be a breach under the organization's response and report policy. But the organization still would have to deal with the complaint by taking the following actions:

- finding out the facts;
- taking appropriate action;

- notifying the individual of the action; and
- keeping records of the complaint and its disposition for six years.

Conclusion

Because HIPAA enforcement is complaint driven, handling complaints in-house rather than having HHS handle them is critical. Proper handling of complaints requires (1) competent people in key positions to handle complaints; (2) an effective reporting and response procedure; (3) appropriate measures to mitigate any potential harm caused by a security incident, protect the individual who was the subject of the breach, and minimize the covered entity's liability; (4) proper disciplinary action pursuant to a sanction policy to demonstrate that the entity is serious about protecting PHI; and good record-keeping as required by the rules. ■

Jonathan P. Tomes, a shareholder in Tomes & Dvorak, Chartered, is a healthcare attorney. He is the author of numerous books and articles including THE COMPLIANCE GUIDE TO HIPAA AND THE HHS REGULATIONS (3rd ed. 2006). He is also President of EMR Legal, a HIPAA consulting firm with clients ranging from state government agencies, such as the Alabama Department of Mental Health and Mental Retardation; county governments, such as Wayne County, Michigan (Detroit); hospitals, physician practices, long-term care facilities, and business associates of covered entities.

will not be limited to seeking repairs from contract suppliers.

For suppliers of oxygen equipment and capped rental equipment, the final rule provides for a minimum number of monthly rental payments to contract suppliers who assume responsibility for furnishing such equipment, after the rental period has begun, to beneficiaries who are no longer renting from their previous suppliers. If a beneficiary who is renting capped rental equipment switches from a noncontract supplier to a contract supplier, the new contract supplier will receive at least 13 months of rental payments, regardless of the number of monthly rental payments Medicare previously made to the prior supplier, assuming the item remains medically necessary. Similarly, a new contract supplier of oxygen equipment will receive at least 10 months of rental payments.

The final rule will be published in the *Federal Register* on April 10, 2007, and will be issued as a pamphlet and available online as part of an upcoming report. ■

CMS Release, April 2, 2007.

Tenet settles allegations it misled investors

by Stacey Fahrner, J.D., M.P.H., Contributing Editor

Tenet Healthcare Corporation announced on April 2, 2007, that it entered into a $10 million civil settlement with the Securities and Exchange Commission (SEC) to resolve allegations that the company failed to disclose to investors that strong earnings growth from 1999 to 2002 was driven by exploiting of a loophole in the Medicare reimbursement system, a practice known as "turbocharging."

Turbocharging. Medicare compensates hospitals at a higher rate for treating extraordinarily sick patients through outlier payments, which are calculated using a cost-to-charge ratio. Outlier payments can be artificially inflated by increasing the hospital's gross charges. According to the SEC complaint, Tenet's management team calculated the precise increase to gross charges needed to boost its revenue to a level that would allow Tenet to reach its earnings targets. Between 1999 and 2002, Tenet's outlier revenue tripled and accounted for over 40 percent of the company's earnings. The scheme was discovered in 2002 when an analyst at an investment banking firm published a report suggesting that the company's financial success was a result of manipulating Medicare outliers. Tenet shareholders lost an estimated $11 billion in market capitalization as a result of the scheme.

In June, 2006, Tenet settled a suit with the Department of Justice (DoJ) for $900 million regarding the turbocharging scheme (See "Tenet settles FCA allegations for $900m," Vol. 9, Issue 14, July 10, 2006.). In addition, Tenet entered into a five-year corporate integrity agreement with the Office of Inspector General (OIG), which contained provisions requiring Tenet's board of directors to undertake a review of the effectiveness of Tenet's compliance program (See "Tenet CIA includes board of director review," Vol 9, Issue 21, Oct. 16, 2006).

SEC settlement. Unlike the complaints issued by the DoJ and OIG, the SEC's allegations do not stem from the Medicare scheme itself, but from Tenet's failure to disclose the impact on earnings. As a result, the SEC claims Tenet misled investors by creating a false impression of the true reasons behind its financial performance.

Tenet response. According to Tenet, the company has been operating under new management and a new board since 2003. Tenet's general counsel, Peter Urbanowicz, stated that "Tenet today is virtually a new company. We are proud of the progress we have made in our commitment to quality care for our patients and transparency in all our operations." ■

Securities and Exchange Commission v. Tenet Healthcare, United States District Court , Central District of California, CV-07-2144, April 2, 2007; Tenet Healthcare Press Release, April 2, 2007.

Fraud & Abuse

Judge imposes $334 million fraud judgment on Medicaid HMO

by Valerie L. Witmer, J.D., Contributing Editor

A federal judge has awarded over $334 million in a fraud lawsuit against the Medicaid health maintenance organization, Amerigroup Illinois, and its parent company, Amerigroup Corporation. The verdict amounts to one of the largest ever fraud judgments against a Medicaid contractor and the largest civil verdict in the history of the Illinois Attorney General's office.

Fraud scheme. From 2000-2004, Amerigroup received hundreds of millions of dollars to fund a Medicaid managed care health plan to help low income pregnant women who had inadequate prenatal care. However, Amerigroup spent less than half of the funds they were paid by state and federal governments on providing health care.

In October, the jury in the case found that Amerigroup illegally avoided providing care to pregnant women and others with expensive health conditions, while continuing to receive state and federal funds that were paid with the understanding that Amerigroup would not discriminate on the basis of health status or need for health services. As a result of Amerigroup's discriminatory practices, certain individuals were denied full access to health care coverage, and the federal and state governments overpaid Amerigroup by millions of dollars.

Judgment. As a penatly for Amerigroup's fraudulent conduct, the judge tripled the jury's original award of $48 million and assessed additional penalties totaling in excess of $190 million, for a total judgment amount of $334,365,000.

The judge stated that he was "convinced that [Amerigroup's] conduct was egregious and calculated" and that [its] actions constituted an "institution-wide goal to fleece [Amerigroup's] pockets at the expense of the government, the Medicaid system, and the avoided pregnant women." ■

Illinois Attorney General Press Release, March 13, 2007.

In the News

Senator introduces universal health care bill

House Ways and Means Health Subcommittee Chairman Pete Stark (D-Calif.) on March 29, 2007, introduced "The AmeriCare Health Care Act," a bill to provide health insurance to all U.S. residents. Under the act, people would either be covered through their employer or through AmeriCare, a new program that would use Medicare's existing administrative infrastructure, but provide a comprehensive prescription drug benefit, mental health parity, pediatric care, and family planning and pregnancy-related services. Employers, individuals, and states would finance the program through contributions. According to The Commonwealth Fund, a health policy organization, the net impact on health care costs would be a $60.7 billion reduction in overall spending

CCH Washington Bureau, March 29, 2007.

S. C. to resolve FCA public disclosure question

The U.S. Supreme Court will hear the case of *United States ex. rel. Bly-Magee v. Premo et. al.* to resolve whether disclosures by state and local governments constitute public disclosure under the "public disclosure bar" of the federal false claims act (FCA), which prevents *qui tam* relators from maintaining a false claims suit based on information that is considered public knowledge. Specifically, the court will determine whether the phrase "administrative. . . report, hearing, audit, or investigation" includes disclosures by state and local governments.

United States ex. rel. Bly-Magee v. Premo et. al., Petition for Writ of Certiorari, United States Supreme Court, March 16, 2007, Health Care Compliance Reporter ¶800,301.

CMS announces NPI contingency plan

CMS announced that it is implementing a contingency plan for covered entities who will not meet the May 23, 2007, deadline for compliance with the National Provider Identifier (NPI) regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). "The enforcement guidance released today clarifies that covered entities that have been making a good faith effort to comply with the NPI provisions may, for up to 12 months, implement contingency plans that could include accepting legacy provider numbers on HIPAA transactions in order to maintain operations and cash flows." said CMS Acting Administrator Leslie V. Norwalk.

CMS Press Release, April 2, 2007.

NY names Medicaid inspector general

New York Governor Eliot Spitzer announced the nomination of James G. Sheehan to serve as New York State Medicaid Inspector General. Sheehan currently serves as an Associate U.S. Attorney for Civil Programs in the Eastern District of Pennsylvania and is responsible for several high-profile recoveries on behalf of the government. He led the investigation against Medco Health Solutions, which resulted in a $155 million recovery. He also served as lead counsel in *United States v. SmithKline Beecham Clinical Labs*, which resulted in a $332 million recovery. As Medicaid Inspector General, he will oversee the fraud and abuse enforcement activities of New York's $50 billion Medicaid program.

New York Governor Press Release, April 6, 2007.