CCH Healthcare Compliance LETTER

Volume 7, Issue 7 www.cchgroup.com April 5, 2004



# CMS releases details on specialty hospital moratorium

## by Sharon Sofinski, Coordinating Editor

The Centers for Medicare & Medicaid Services (CMS) has announced details of its plan to implement an eighteen-month moratorium on physician investment in and referrals to certain specialty hospitals. The moratorium was enacted by Sec. 507 the Medicare Prescription Drug, Improvement and Modernization Act of 2003 (MMA) (PubLNo 108-173) and became effective on December 8, 2003. It will expire on June 8, 2005.

The moratorium applies to specialty hospitals that are primarily or exclusively engaged in the care and treatment of:

- patients with cardiac or orthopedic conditions,
- patients receiving surgical procedures, or
- patients receiving any other specialized category of services that CMS may designate.

The following types of specialty hospitals are excluded from the moratorium:

- psychiatric hospitals,
- rehabilitation hospitals,
- children's hospitals,
- long-term care hospitals,
- cancer hospitals that are not paid under the inpatient hospital prospective payment system, and
- grandfathered specialty hospitals.

Grandfathered specialty hospitals are those that were in operation before or under development as of November 18, 2003. In determining whether a hospital was under development as of that date, the MMA directs CMS to consider whether the following had occurred by the date: architectural plans were completed, funding was received, zoning requirements were met, and necessary approvals from appropriate state agencies were received. CMS can also consider any additional evidence that it believes would indicate whether a specialty hospital was under development by the November date. If CMS determines that a hospital was not under development as of November 18, 2003, it is not a grandfathered specialty hospital, and physician investors in that hospital may not refer patients to it until June 8, 2005.

A specialty hospital can obtain a determination as to whether it was under development as of November 18, 2003 by submitting a written advisory opinion request to the CMS central office. Specialty hospitals with a Medicare provider agreement in place as of the November date are deemed to have been in operation and do not need to request a determination from CMS.

The notice containing the moratorium details can be found on the CMS website at http://www.cms.hhs.gov/manuals/pm_trans/R62OTN.pdf. ■

*CCH Chicago Bureau, March 24, 2004*

## Stark II Phase II Interim Final Rule released

**by Sharon Sofinski, Coordinating Editor**

The Centers for Medicare & Medicaid Services (CMS) has issued Phase II of the physician self-referral law (commonly known as Stark II). The new regulations were published in the Federal Register on Friday, March 26, 2004 and will be effective on July 26, 2004.

Stark II prohibits a physician from referring Medicare and Medicaid patients for certain designated health services to entities with which the physician (or a member of the physician's immediate family) has a financial relationship. The law also prohibits entities from billing for services resulting from a prohibited referral.

According to CMS Acting Administrator Dennis Smith, Phase II of the regulations "will protect Medicare and Medicaid beneficiaries from potentially abusive referrals, while accommodating legitimate business and financial arrangements, including those that enhance the emerging national health information infrastructure." Smith stressed that the new regulations will not impose additional burdens on physicians who are trying to structure their business arrangements to comply with the law. Phase I of Stark II, published in January 2001, defined many of the terms in the statute, interpreted some of the major statutory exceptions, and created a number of new regulatory exceptions.

**New exclusions created.** Phase II includes CMS's response to comments it received on the Phase I regulations, addresses issues not covered in Phase I, and creates several new regulatory exceptions for nonabusive financial relationships. The new regulations includes a new exception for community-wide health information systems, limited exceptions to allow physicians to refer to immediate family members in rural areas in certain circumstances where no other physician is available, and an exception to exempt hospital payments to retain a physician who would otherwise leave a health professional shortage area. Exceptions have also been created for Medicaid managed care plans; professional courtesy arrangements; certain inadvertent and temporary lapses in compliance with an existing exception; and charitable contributions by physicians to entities that furnish designated health services.

According to CMS, the exception for community-wide health information systems will help encourage providers to use electronic health records and thus "have very positive advantages for American health care by enhancing the country's movement toward a national health information infrastructure that will serve consumers, patients, health care providers and public health professionals."

**The regulations "will protect Medicare and Medicaid beneficiaries from potentially abusive referrals, while accommodating legitimate business and financial arrangements, including those that enhance the emerging national health information infrastructure."**

In response to comments on Phase I, CMS has also revised the definition of compensation that is "set in advance" to permit certain common percentage compensation arrangements; made the academic medical centers exception more flexible; expanded the medical staff incidental benefits exception to include facilities other than hospitals; and expanded the exception for certain dialysis-related drugs to include more drugs used in connection with dialysis treatment. The hospital ownership exception has been revised to reflect the new 18-month moratorium on physician ownership of specialty hospitals, which was recently enacted by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003. The Phase II regulations also address statutory exceptions for physician investment interests in publicly traded securities and mutual funds and physician ownership of rural providers and hospitals.

**Comments.** Comments on the Phase II regulations are due by June 24, 2004. For more information see CMS's press release at http://www.cms.hhs.gov/media/press/release.asp?Counter=985. ■

*CCH Chicago Bureau, March 26, 2004*

CCH Healthcare Compliance LETTER

**Managing Editor**
*Yvonne Kanak*

**Coordinating Editors**
*Angela Fanelli, J.D.*
*Sharon Sofinski*

**CCH Washington Bureau**
*Paula Cruickshank*
*DOJ, FTC–John Scorza*
*SEC–Peter Feltman*
*Health Law–Catherine Hubbard*
*Tax–Jeff Carlson, David Hansen*

**Designer**
*Craig Arritola*

Comments from readers are welcome and should be directed to Sharon Sofinski at SOFINSKS@CCH.COM, Tel. 847-267-7860, Fax 847-267-2514. Customer service inquiries should be directed to 800-449-9525.

*CCH Healthcare Compliance Letter* is published 24 times a year by CCH INCORPORATED, 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 Healthcare Compliance Letter*, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A.

## Clinic operators, physician convicted of fraud

**by Sharon Sofinski, Coordinating Editor**

Two operators of physical therapy clinics have been convicted of conspiracy and Medicare fraud, the U.S. Attorney for the Southern District of Texas has announced.

Monet Selders and Tamara Fitzgerald operated two clinics—Infinity Health and Medical Group and Medical Management Services. Both admitted to fraudulently billing Medicare for more than $2.6 million over a 6-month period in 1999. The fraud included billing Medicare for services that were not performed, for evaluations that were not performed by a physician, and for services that were performed by unlicensed technicians in a patient's home without a physician's supervision. The defendants also admitted that they hired a foreign medical student who was not a physician to perform patient evaluations.

The investigation into the fraudulent activities also found that Medical Management Services sometimes operated out of the same office as Infinity Health, did not have any technicians on staff, and submitted bills to Medicare for Infinity patients without their knowledge. Furthermore, Selders and Fitzgerald paid individuals kickbacks from amounts collected from Medicare for patient referrals.

Both women pled guilty to the charges and face a maximum 15-year prison sentence and a $500,000 fine.

Selders also submitted $1.1 million in fraudulent claims in 1999 for another clinic she operated, Care Group 2000. In a related case, Selders's sister, Kimberly Selders, was convicted of defrauding Medicare of $500,000 in connection with her operation of a the Mirage Medical Group physical therapy clinic. The U.S. Attorney's press release on this case is at http://www.usdoj.gov/usao/txs/releases/March2004/040304-selders.htm.

In another fraud case, the U.S. Attorney for the Southern District of Florida announced that Dr. Paul Elliott, D.O., was convicted on twenty-two counts of health care fraud and one count of obstruction of justice.

Elliott was the president and part owner of Doctor's Care Medical Center, Inc., which operated five clinics in Florida. According to the evidence at trial, Elliott directed the clinics to bill Medicare for comprehensive MRIs performed on patients when MRIs without an injection of contrast medium were actually performed, in order to receive a higher reimbursement. He also billed Medicare for electromyography (EMG) tests that had not been performed. Each type of fraud occurred more than 200 times.

**The fraud included billing Medicare for services that were not performed, for evaluations that were not performed by a physician, and for services that were performed by unlicensed technicians**

Elliott was convicted of obstruction of justice for submitting to the U.S. Secret Service more than 150 patient records that he had altered to show that the EMGs had been performed when in fact they had not. Elliott faces a maximum 10-year prison sentence and $250,000 fine for the health care fraud counts, and a 20-year sentence and $250,000 fine for obstruction of justice. The U.S. Attorney's press release is at http://www.usdoj.gov/usao/fla/Elliott2.html. ■

*CCH Chicago Bureau, March 26, 2004*

### Letters to the Editor

The CCH Healthcare Compliance team welcomes comments or questions regarding articles published in the CCH Healthcare Compliance Letter. Send comments to Sharon Sofinski, Coordinating Editor, at sofinsks@cch.com. For more information about the CCH Healthcare Compliance Portfolio visit our online store at http://health.cch.com.

# The evolution of risk management to corporate compliance and beyond

by Sanford V. Teplitzky, Esq. and Steven R. Smith, Esq.

*Risk management is in the process of evolving. Both the scope of what is included in the concept of risk management and the risks that face most hospitals[1] have greatly expanded in recent years. This evolution is occurring in response to changes that have taken place in the broader healthcare environment. The result of this evolution is that, in the interests of both the hospitals and their patients, hospitals need to view and manage the risks that they face from an organization-wide perspective and not as isolated issues to be confronted on a department by department basis.*

The traditional role of the risk manager was, not surprisingly, tied to the traditional concept of risk. "Risk" has been defined as "the chance of injury, damage or loss"[2] and has been closely aligned to concepts of loss in the context of insurance and safety matters. Therefore, the traditional role of the risk manager was to manage the risk of loss from events that were insured against. This may have meant simply working with an insurance broker to facilitate the placement of insurance policies (facility professional liability and general liability) to cover such insured losses or a more proactive approach to manage these risks. However, even the proactive approach was traditionally limited to a relatively limited menu of risks such as falls and medication errors.

The healthcare environment that is compatible with this concept of risk management has markedly changed. That overall change has been driven by several environmental factors that have significantly expanded the risks that must be managed within a hospital. Among those factors are:

- the spread of managed care payment systems as a significant part of the reimbursement structure;
- the rapid increase in electronic communications capabilities;
- the expansion by the federal government of regulation of the health care industry; and
- the emphasis on patient safety initiatives.

As a result of these changes in the healthcare environment, hospitals face a much wider range of risks that require a coordinated approach to management if they are to be effective. Each of these changes in the healthcare environment, their impact on the risks that hospitals face and how they have helped to shape the approach to risk management are briefly reviewed below.

## Managed Care Payment Systems

Managed care payment systems ("Plans") seek to control the cost of health care by controlling the utilization of, and access to, health care. This is accomplished by restricting the number of facilities in the Plan's network (i.e., those facilities with which the Plan contracts to be available to members), by including provisions in hospital contracts that require hospitals to obtain prior authorization from the Plan before providing treatment to members and by imposing limits on authorized lengths of stay. These requirements create a couple of new kinds of risk for hospitals. First, an organizational risk of financial loss is created as a result of the hospital's either being excluded from the Plan's network or from its noncompliance with the preauthorization and length of stay requirements established by the Plan. Second, an organizational risk of loss from negligence is created as a result of the potential tension between adhering to the Plan's prescribed plan of care or authorized length of stay and the true medical needs of the patient. Too often, Plans may not adequately consider a physician's request for additional authorized days or other treatment for the patient. When this happens, hospitals and doctors face the choice of listening to the medical advice being provided for the patient and risk nonpayment, or discharging the patient and risk a negligence action if their concerns prove to be well-founded and the patient has an adverse outcome.

In the absence of Plans, these risks simply do not exist. Patients are either insured or uninsured. The financial risk of the uninsured is the same regardless of the presence or absence of Plans. For insured patients, their insurance pays for what is done. As Plans have become an ever larger part of the system of reimbursement for hospitals, these risks have become proportionately larger concerns in the overall functioning of the hospital.

## Electronic Communications

We live in an age where the ability to communicate and work in an advanced electronic and technological environment is taken for granted. We use email for a vast amount of communication both within and without our work environments.

We have access to the Internet, which in turn provides us with access to information and research from government agencies and regulatory bodies on a moment's notice. Cell phones are commonplace (and perhaps indispensable) in our workplaces. Computer and software advances have completely transformed our ability to compile, analyze, sort and categorize information into easily understood and user friendly formats. All of this means that we are now able to collect information more easily, communicate that information to each other more easily and more frequently, and put that information into different formats for use in different settings.

This has not always been the case. Before email there was nothing other than regular mail or internal rounds of mail sent inside a hospital. There was no Internet so research was done only if one had access to the materials and then through a labor-intensive process. Cell phones in the workplace were non-existent, which meant that if a fellow employee was not at his or her desk or station then a message (usually manually) had to be taken so the person could call back. Desktop computers, if they existed, were bulky, slow, and inefficient in the sense that there was not much sophisticated software available for the use of risk managers.

The evolution of our technology and communications abilities has also given rise to new risks. With the convenience and openness of the Internet comes the potential for the invasion of privacy and the need to protect vital organizational and patient information from "worms" and hackers. Organizations as a whole also have to protect against a loss of productivity and potential liability from the inappropriate use of the Internet by its employees. The same risks are present with email and, in conjunction with the increased access to and utility of computers, additional risks arise such as the ability to quickly and easily access confidential information and send it out by email without notice. These are all risks that need to be evaluated and managed by a hospital in the modern healthcare environment.

## Expansion of Federal Regulation of Healthcare

Today's hospitals have to perform their responsibilities in a virtual maze of regulations and mandates. These laws and regulations add tremendous complexity and expense to the operation of a hospital. Three examples of the impact of such laws and regulations on the healthcare environment are the Emergency Medical Treatment and Active Labor Act (EMTALA), the Health Insurance Portability and Accountability Act (HIPAA) and the increased focus on and enforcement of the fraud and abuse laws.

EMTALA[3] essentially requires that everyone who presents to an emergency department of a hospital requesting treatment for an emergency medical condition must be provided a screening examination and necessary stabilizing treatment or transfer under certain conditions.[4] EMTALA did not break any new ground from the standpoint of the adequacy of treatment received by patients. That subject is still the purview of state negligence actions.[5] EMTALA was enacted to respond to a societal problem of patient dumping.[6] That response was to require essentially all hospitals with emergency departments to treat all persons who present to the hospital for an emergency medical condition in the same way and to impose various other administrative requirements on the hospital in order to allow the government to determine whether the hospital is complying with the requirements of the law.

The administrative simplification provisions of HIPAA[7] were enacted to provide greater protection to the privacy and security of medical records and to provide for the electronic submission of claims for payment for providing health care. These provisions apply to health care providers who transmit health information in electronic form in connection with certain transactions.[8] HIPAA creates important new protections for the privacy and security of medical records but these protections are necessary only because the environment has changed into one that is dominated by the electronic transmission of information.

The fraud and abuse laws[9] provide important protections against fraudulent and other abusive behavior by healthcare providers. The increased focus on these laws has made healthcare providers aware of the potential for significant penalties to be imposed if they were violated. That awareness was, at least in part, responsible for the movement towards the development of compliance plans for hospitals as a result of the beneficial effect that an effective compliance plan can have on penalties imposed on an organization as a result of the violation of these laws.[10] The development of compliance plans necessarily caused hospitals to focus on risks throughout the organization with the emphasis being on the recognition of standards and compliance therewith.

Each of these laws and regulations represent a governmental response to important issues that have arisen in the delivery of healthcare. They have also increased the level of complexity of the healthcare environment and created new risks for the organizations that operate in that environment. These risks are largely the risks associated with non-compliance. The management of those risks entails the creation of policies, the orientation and education of staff on those policies and the auditing and monitoring of the implementation of the policies. These responsibilities extend from the emergency department (and other areas of the hospital) for EMTALA, the health information management department (and all other areas of the hospital) for HIPAA, and most areas of the hospital, especially the business office and hospitals' relationships with physicians, for the fraud and abuse laws.

## Patient Safety

The emphasis on patient safety in hospitals has dramatically altered how patient care delivery systems are viewed. Patient safety activities are generally focused on looking at the process by which things get done for patients, as opposed to who does something, and then looking further to see flaws in that process and how those flaws can be corrected. It recognizes that human beings make mistakes and that those mistakes are often the result of failures in systems.

This requires much work. Open communication is essential both among staff members and with the patient. Detailed analyses of problem areas have to be conducted in order to determine the root cause of the problem and how systemic issues contributed to the existence of the problem. Finally, new solutions have to be devised that eliminate the existing systemic issues without creating new ones. Through the analysis and improvement of the processes and systems involved in the care of patients, patient safety initiatives require a hospital to realize that it exists as a single organization for the purpose of taking care of patients and that its various departments cannot be viewed as existing in a vacuum.

The movement towards patient safety is a given. Hospitals are required by the Joint Commission on the Accreditation of Healthcare Organizations to have an integrated patient safety program.[11] States are considering the incorporation of patient safety initiatives into their regulatory schemes for hospitals.[12] These changes clearly are shaping the manner in which hospitals are viewing and managing their risks.

## The Next Step

Hospitals face a much wider range of risks to the organization than was the case in the past. The expansion of risks has largely been driven by the changes that have taken place in the healthcare environment. Some of those changes have been briefly reviewed above. Given that these new risks exist, where do they reside in the hospital setting and who has ownership of the management of those risks?

One answer is to continue to treat the hospital as being made up of independent component parts that function largely independent of each other. In this model, one or more departments of the hospital would likely be assigned the primary responsibility to confront the risks presented for each of the areas previously reviewed. The persons in charge of those areas would have to develop policies and procedures to address the risk concerns for the organization. Most likely, the persons in charge of each of those areas will be different and they will not have the organizational "reach" to pull others into the process.

As more organizations are discovering, the alternative is to view hospitals as an integrated system of care. This is consistent with the changes that have occurred in the healthcare environment and with sound management practice, and is an accurate reflection of the real liabilities of the hospital. Regardless of who is performing what function, hospitals, as organizations, are responsible for the care that they provide to patients. Tort principles recognize this liability through the concept of apparent or ostensible agency.[13] Hospitals need to get on board with the idea that they are going to be held to a standard of an integrated organization so they need to manage their risks like one.

Under this model, a senior person in the organization with direct reporting lines to the President and/or Board is responsible for all of the risks of the organization.[14] This person is charged with looking at the organization as an integrated system of care and bringing interdisciplinary teams of people together to dissect, analyze and create new systems to respond to the risks faced by the organization. This requires support at the highest levels of the organization in order to allow the person responsible to break through the inevitable barriers that will be confronted. The foothold taken by patient safety and compliance activities is clearly a stepping stone towards a more global view of hospitals as integrated organizations. As the environment continues to change, this will expose even more risks and force more organizations to view themselves in this light. The result of understanding the total risks of the hospital and working in an integrated fashion to manage those risks will be a better hospital organization and better patient care.

*Mr. Teplitzky is a Principal and Chairman of the Health Law Department of Ober, Kaler, Grimes & Shriver and is resident in the Baltimore office of the firm. Mr. Teplitzky offers his experience to clients—typically large health care companies and delivery networks—who seek help with fraud and abuse problems and representation in federal or state investigations. Mr. Teplitzky can be contacted at (410) 347-7364 or by email at teplitzky@ober.com. Mr. Smith is a Principal of Ober, Kaler, Grimes & Shriver and is resident in the Washington, D.C. office of the firm. Mr. Smith was the former Senior Vice President & General Counsel for a significant health care system where he was responsible for, among other things, insurance and risk management issues. He has more than twenty years of experience focusing on general corporate matters and employment and labor law issues in a health care setting. Mr. Smith can be contacted directly at (202) 326-5006 or by email at ssmith@ober.com.*

1 This article refers to all health care facilities as "hospitals" since they typically have greater risk management presence than other health care facilities. However, this is not meant to imply that these comments do not also apply to other health care facilities.

2 *Webster's New World Dictionary of the American Language,* Second College Edition, 1976.

3 42 USC §1395dd et seq.

4 42 USC §1395dd (a) and (b).

5 See, e.g., Bryan v. Rectors and Visitors of University of Virginia, 95 F.3d 349, C.A. 4 (Va.) (1996).

6 See, 68 Fed. Reg. 53222, 53223.

7 42 USC §1320d et seq.

8 42 CFR §160.102 (a).

9 See, e.g., The Federal Civil False Claims Act, 31 USC §3729; The Anti-Kickback Statute, 42 USC §1320a-7b; and the "Stark" Law, 42 USC §1395nn.

10 United States Sentencing Commission, Guidelines Manual, §8C2.5(f) (Nov. 2003).

11 Standard LD.4.40, Comprehensive Accreditation Manual for Hospitals (2004), Joint Commission on Accreditation of Healthcare Organizations.

12 See, e.g., Code of Maryland Regulations 10.07.06.01 et seq.

13 E.g., Mehlman v. Powell, 281 Md. 269 (1977).

14 This position is often known as the Chief Risk Officer.

## Rogue employees present some of the greatest threats to privacy, attorney says

**by Catherine Hubbard, MA, Contributing Editor**

Employees who expose protected personal health information (PHI) will present hospitals and other covered entities with some of the most difficult challenges in complying with the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules, according to Edward Shay, a partner at Post & Schell's Philadelphia office.

Courts are also indicating they will not hold an organization harmless when rogue employees disclose PHI, Shay said during a March 23 audio conference sponsored by the Health Care Compliance Association. "You have to assume the worst and you have to do everything you can to mitigate," he said.

In *Foster for J.L. v. Hillcrest Baptist Medical Center*, an employee removed a patient's file from the premises and showed it to a person who allegedly had abused the patient. The court did not dismiss the case as Hillcrest had hoped, Shay noted.

"If an employee acts out, you have to be able to show how you enforce the policies and procedures and monitor compliance," said Shay. "If you can't do that, you're going to have to go to trial on these kinds of cases," he warned.

Shay joked that he sometimes refers to HIPAA as "The privacy officers' full employment act." However, he warned, "If you're a health care covered entity under the HIPAA privacy rule and you have adopted policies and procedures, this is not a one and done exercise. You have to enforce those procedures."

The Health and Human Services Department Office of Civil Rights logged about 3,000 complaints under HIPAA last year, said Shay. Most of the complaints either were resolved quickly or could not be addressed with the privacy rule, but a handful were referred to the Department of Justice for investigation, he said. "The government expects there to be quite a few more complaints in the future," he said, noting that for fiscal 2004, OCR has the resources to handle 21,000 complaints.

**Use mitigation.** "Compliance officers can make a major contribution in the context of privacy litigation through the exercise of mitigation," Shay said. The recent class action lawsuit involving TriWest Healthcare Alliance Corp. (*Stollenwerk v. TriWest*) is a classic case of where mitigation was sufficiently successful, he said. The plaintiff's class could not show harm and in the absence of a showing of harm, the court dismissed the case. "Mitigation works," said Shay, "It's an area we all need to spend a lot of time on and think very carefully about." Privacy officers should get involved when they first see the warning signs of a privacy dispute, he suggested.

**"If you're a health care covered entity under the HIPAA privacy rule and you have adopted policies and procedures, this is not a one and done exercise. You have to enforce those procedures."**

In *TriWest*, a thief broke into the company's facilities and stole a laptop containing unencrypted PHI on more than 500,000 military personnel and their dependants. "It was a major breach of security," Shay said. The court dismissed a class action lawsuit for breach of security. "The court was of the view that there was no harm shown," he explained.

**Litigation trends.** One of the greatest legal exposures exists in employment cases where an employee has been terminated. "Employment-driven disputes have the potential for a lot of difficulty for the covered entity," said Shay. These could include health plan denials, the migration of PHI from the plan to the employer and its use in the employment process. "Even though that is prohibited under the privacy standards, I suspect that will happen on occasion. People have big ears and sometimes bigger mouths and sometimes word gets around," he cautioned.

Another source of lawsuits, Shay predicted, will come from people who are locked in medical malpractice suits. "They are looking for any handhold that will give them an advantage," he said. "Complaining to the secretary will soon become the opening move in some of these medical malpractice cases once the plaintiffs' bar figures out how to sue that particular avenue of compliant," he warned.

Likewise, any breach of PHI privacy that falls into the category of identity theft will be loaded with potential for both complaints and problems, Shay predicted. "The TriWest case is a classic identity theft case," he added. If there is an actual showing of harm, he said, "you could see the importance of ID theft exposures." Already there have been several cases where employees have stolen credit card information from either the hospital's paper or computer records. "Those cases have the potential for a lot of agony for the covered entity," he said.

Currently, there are more procedural HIPAA cases than there are substantive cases because the courts are struggling with the process of change and with questions like how to serve a subpoena under the rule and when it can use an authorization. "Those kinds of questions tend be the focus of litigation," he said.

Furthermore, trial lawyers are interested in class action suits in the area, but haven't quite worked out the business model for taking on these kinds of cases, Shay said. "We have not seen the major wave of privacy class action suits we predicted when we first had a look at the privacy rule," he said. For example, lawyers haven't figured out how best to profit from the cases, he said. "If you are a plaintiffs' class action lawyer, the one thing you want to understand before you start a lawsuit is how you're going to be paid at the end," he said.

Meanwhile, there is little incentive for lawyers to take on individual

## Human Resources

### EEOC sues nursing home for bias against employee with HIV

**by Robyn J. McCain, J.D., Contributing Editor**

The U.S. Equal Employment Opportunity Commission has filed a disability discrimination suit against Maple Lawn Nursing Home in Palmyra, Missouri, for unlawfully terminating an employee because she was HIV-positive.

In June 2002, Maple Lawn Nursing Home fired a certified nurse's aide when she reported to the nursing home administrator that she had tested positive for HIV. The EEOC's suit alleges that this termination violated the Americans with Disabilities Act. The employee did not perform duties which could result in blood-to-blood contact with patients. According to the Centers for Disease Control, HIV-infected health care workers who do not perform invasive procedures and who adhere to universal precautions, such as wearing gloves, pose no risk for transmitting HIV to patients.

The EEOC's complaint, filed in the U.S. District Court for the Eastern District of Missouri against Marion County Nursing Home District, Inc., doing business as Maple Lawn Nursing Home (case no 4:04cv00298snl), seeks lost wages, compensatory and punitive damages, and reinstatement for the nurse's aide.

"We have come too far in our understanding of how HIV and AIDS are transmitted to expect this type of discrimination to occur, especially in a medical setting," said Lynn Bruner, Director of the EEOC's St. Louis District Office. "The EEOC will continue to litigate these cases until all employers are educated about this disability." ■

*CCH Chicago Bureau, March 13, 2004*

## HIPAA (cont.)

clients in HIPAA privacy cases, Shay said. "If you don't have a class action lawsuit, you're not going to have a very big payday," he said, noting that "Privacy cases tend not to involve large economic damages." Many states cap noneconomic damages and the federal government is considering caps as well, he noted. ■

*CCH Washington Bureau, March 26, 2004*

## Quality

### MedPAC asks Congress to reward quality in Medicare

**by Catherine Hubbard, MA, Contributing Editor**

Congress should reward health care organizations that provide high quality care under Medicare, according to Glenn Hackbarth, chairman of the Medicare Payment Advisory Commission. Speaking at a recent House subcommittee hearing, Hackbarth said the Medicare program "can no longer afford for its payment systems to be neutral or negative to quality." He advocated lawmakers put financial incentives for quality directly into the Medicare payment systems.

From 1995 to 2002, rates of adverse events in nine out of 13 categories tracked by MedPAC increased, according to Rep. Nancy L. Johnson, R-Conn., who chaired the House Ways and Means Health Subcommittee hearing. The Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (PubLNo 108-173) included incentives for hospitals to report a variety of health care quality indicators and encouraged e-prescribing to reduce medical errors and improve administrative efficiency, but "more can be done to improve quality," she said.

"In the current technological environment, urging physicians to print neatly is not enough," Johnson said in a release. "We must provide market-oriented incentives that encourage the delivery of quality health care. Without good information, consumers cannot make intelligent choices between physicians, hospitals, or other providers, and better care will not advance," she said.

Carolyn Clancy, director of the Health and Human Services Agency for Healthcare Research and Quality, said the act includes demonstrations to improve chronic illness care and identify ways to reward top performers. She added that the administration "is committed to working with the health care industry and the various stakeholders to improve the quality of care." ■

*CCH Washington Bureau, March 26, 2004*