CCH Health Care Compliance LETTER

Volume 9, Issue 11 health.cch.com May 30, 2006

Drug companies urged by Senators to continue offering PAPs to Part D enrollees

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

Members of the Senate Finance Committee met with executives from pharmaceutical companies on May 11, 2006, to discuss the future of drug company-sponsored programs that help individuals with high prescription drug costs. At the closed-door meeting, senators urged the companies to continue offering patient assistance programs (PAPs) to beneficiaries who enroll in Part D.

"The new Medicare drug benefit does not and should not prevent them from continuing to offer patient assistance programs to Medicare beneficiaries who enroll in Part D," Senate Finance Committee Chairman Chuck Grassley said. "Out-of-pocket costs for hyper-expensive drugs can be an insurmountable barrier for many beneficiaries, even with the new Medicare benefit."

OIG guidance. According to Grassley, the May 15 deadline for Part D enrollment became "an excuse for dropping the assistance that many Medicare beneficiaries rely on." Legal avenues do exist for companies to continue their programs, however. On April 18, 2006, the Office of Inspector General (OIG) released an advisory opinion (see *Heath Care Compliance Reporter* ¶500,138) holding that a pharmaceutical company's patient assistance program that provided free outpatient drugs to financially needy enrollees outside of the Part D benefit posed a minimal risk of fraud and abuse. This advisory opinion expanded on a November 2005 OIG Special Advisory Bulletin (see *Heath Care Compliance Reporter* ¶520,027) that outlined potential approaches for operating a PAP in the new Medicare prescription drug environment.

In an April 21, 2006, letter to the Pharmaceutical Research and Manufacturers of America (PhRMA), the industry trade group that met with members of the Senate Finance Committee on May 11, the senators stressed that the OIG indicated in the Special Advisory Bulletin that it would exercise discretion in taking enforcement actions against pharmaceutical manufacturers operating PAPs in 2006, the first year of the Part D benefit. "These facts make a company's decision to end its PAP as of May 15 seem rather arbitrary," the senators said in the letter.

"Now that the Inspector General has provided some concrete guidance, it's time for pharmaceutical companies to fulfill their obligation," said Senator John D. Rockefeller IV.

Pharmaceutical industry's response. Some pharmaceutical companies said that they plan to continue their programs or parts of their programs. For example, according to the April 21 letter, Merck, Schering-Plough, and AstraZeneca have announced that they will continue their PAPs.

continued on page 2

Wolters Kluwer Law & Business

Anti-kickback (cont.)

Rockefeller, however, urged the companies to do more. "Some companies in recent days have announced that they will continue their PAP programs for Medicare beneficiaries, and I hope more companies follow suit," he said. "But more needs to be done. Many subsidy-eligible Americans will need additional assistance meeting their Medicare drug benefit co-insurance obligations, and I want to make sure that free clinics around the country do not lose access to the drugs they currently receive through PAPs." ■

U.S. Senate Finance Committee News Release, May 11, 2006.

Proposed cost-sharing assistance poses few anti-kickback concerns

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

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

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

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

According to the OIG's advisory opinion, it appears unlikely that donor contributions to the corporation would influence any Medicare beneficiary's selection of a particular provider, practitioner, supplier, or product because the corporation is an independent organization that is not affiliated with any donor and the corporation awards assistance in a truly independent manner that severs any link between donors and beneficiaries. In addition, assistance will be provided based on a reasonable, uniform measure of financial need that will be applied in a consistent manner. Similarly, the corporation's subsidy of premiums and cost-sharing obligations is not likely to improperly influence any beneficiary's selection of a particular provider, practitioner, supplier, or product because beneficiaries will be assisted on a first-come, first-serve basis, a determination of a patient's qualification will be based solely on financial need, and the subsidies will expand beneficiaries' freedom of choice. ■

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

Fraud & Abuse

DME supplier pays $10 M to settle kickbacks, self-referral allegations

Lincare Holdings Inc. and its subsidiary Lincare Inc. (Lincare) one of the nation's largest durable medical equipment suppliers, paid $10 million and entered into a 5-year company-wide Corporate Integrity Agreement (CIA) with the Office of Inspector General (OIG) to resolve allegations that it paid illegal kickbacks and violated the physician self-referral law, HHS Inspector General Daniel R. Levinson announced on May 15, 2006. The settlement is the largest ever for OIG under its civil monetary penalty authorities.

Self-referral allegations. OIG alleged that Lincare, which is headquartered in Clearwater, Florida, engaged in a nationwide scheme to pay physicians kickbacks to refer their patients to Lincare. Lincare gave referring physicians items such as sporting and entertainment tickets, gift certificates, rounds of golf, golf equipment, fishing trips, meals, advertising expenses, office equipment, and medical equipment. The illegal kickbacks also came disguised as payments pursuant to purported consulting agreements, such as Medical Director Agreements. OIG also alleged that Lincare violated the self-referral law by accepting referrals from parties to the illegal consulting agreements.

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.

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

Designer
Don Torres

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.

"This significant settlement is an important example of OIG's continuing effort to eliminate illegal kickback practices and violations of the Self-Referral Law," Levinson said. "OIG will continue to pursue aggressively those who undermine the integrity of the Medicare program."

Under its civil money penalties authority, OIG may impose a penalty of up to $50,000 per illegal kickback and damages of up to three times the amount of the kickback. Under the self-referral law, OIG may impose a penalty of $15,000 for each item or service that was billed to a federal health care program pursuant to a prohibited referral as well as an assessment of up to three times the amount claimed. Under both the anti-kickback and self-referral provisions, OIG may exclude a provider for violations. ■

OIG News Release, May 16, 2006.

Physical therapy billing patterns suggest vulnerability to abuse

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

A random sample of 70 physical therapy line items revealed that 91 percent of physical therapy billed by physicians and allowed by Medicare during the first six months of 2002 did not meet program requirements, resulting in $136 million in improper payments. Furthermore, according to the Office of Inspector General (OIG), aberrances in physicians' billing patterns and unusually high volumes of claims suggested that physical therapy is vulnerable to abuse.

Medical necessity and documentation. Based on the OIG's medical review, 26 percent of the therapy during this period, totaling $33 million, was not medically necessary. Medical reviewers found that there were no objective bases for care, no identified outcomes, and no change in the patients' conditions to justify ongoing therapy. In addition, physicians did not provide substantiating documentation for 34 percent of the services billed to Medicare.

Incomplete plans of care. Fifty-seven percent of the services were furnished under incomplete plans of care or had no plan of care documented. The incomplete plans did not contain information concerning the amount, frequency, or duration of the therapy, or physician certification. When projected to the national population of therapy billed by physicians, the services furnished without a plan of care or under an incomplete plan of care represent $87 million allowed by Medicare during the first six months of 2002.

Quality of services. Because of inadequate documentation, reviewers could not assess the quality of care for 33 of the 54 records they reviewed. The 12 records that contained sufficient documentation caused the reviewers to question the quality of care and note that some services lacked an objective basis for care. In addition, most medical records did not indicate the skill level of the individual who rendered the physical therapy.

Vulnerability to abuse. OIG also identified unusually high volumes of claims and aberrances in physicians' billing patterns, both of which suggest that physical therapy is vulnerable to abuse. For example, for 13,090 beneficiaries, Medicare allowed at least $5,000 each in physical therapy services billed by physicians in 2004, while Medicare allowed a median of only $305 each for the entire beneficiary population for the same time period.

"Incident-to" rule. In addition, based on the medical record documentation provided, OIG could not determine whether physicians were directly supervising staff rendering the physical therapy services, as required by the "incident-to" rule, or even whether direct supervision was physically possible for physicians that billed dozens of beneficiaries daily. That there is no limit on the number of staff that a physician can supervise concurrently could partially account for the noncovered and undocumented care.

Recommendations. OIG recommended that CMS consider revisions, clarifications, and further study of the "incident to" rule to ensure that Medicare beneficiaries are receiving skilled services from appropriately trained and licensed staff and that the services meet professionally recognized standards of care. Furthermore, according to the OIG, the requirements for physician therapy rendered in physicians' offices should not differ from the requirements for therapy rendered in other settings. ■

OIG Report, OEI-09-02-00200, April 6, 2006, Health Care Compliance Reporter, ¶530,398.

Response plan key to mitigation of security breach

by Catherine Hubbard, M.A., Contributing Editor

Medical identity theft is a crime that can cause great harm to its victims, according to a report entitled "Medical Identity Theft: The Information Crime That Can Kill You," issued by the World Privacy Forum on May 3, 2006.[1] *"Victims do not have the same recourse and help for recovery from medical identity theft as do victims of financial identity theft." Identity theft may be carried out by criminals, doctors, nurses, hospital employees and others, the report noted.*

Victims can be plagued by the repercussions of medical identity theft for years, according to Pam Dixon, author of the report and Executive Director of the World Privacy Forum. Medical identity theft occurs when someone uses a person's name or insurance information to obtain health services or to make false claims. It often results in erroneous or falsified medical records. The report also states that falsified information in medical records can lead to the wrong medical treatment and the exhaustion of health insurance; victims could become uninsurable for both health and life insurance. In addition, victims may fail physical exams for employment due to the presence of diseases in their health record that do not belong to them.

"One of the biggest challenges is putting together a response plan quickly."

Responding to a breach. Organizations must establish plans to prevent and mitigate security breaches, according to Benjamin Butler, a partner at Crowell & Moring, Washington, D.C., and member of the firm's Health Care Group. "The more an organization can do before a breach occurs to facilitate a rapid response, the better shape it'll be in when an event does happen," he added during an interview on March 31, 2006.

"One of the biggest challenges is putting together a response plan quickly," Butler said. "The clock starts ticking when you find out that you've had an event that may have exposed somebody's information to a potential identification (ID) theft."

An organization's response depends in part on the state law governing it. In the past two years, many states have adopted laws governing notifications of security breaches; however, those laws vary greatly in terms of when a notification is required, and which types of organizations are obligated to comply. The chart on page 6 provides a summary of current state security breach notification laws including a description of entities that are covered and entities that are exempt.

State security breach laws. Identity theft in the form of theft of patient records and employee laptops has drawn the attention of state lawmakers, who are calling for action. Roughly half of states require entities, including health care organizations, to notify customers affected by a security breach.

State security breach notification laws require organizations to alert potential ID theft victims when their information is stolen or missing, particularly when that information includes a name plus a Social Security number (SSN), driver's license number or account number and passcode. "It's a relatively narrow category of information that is at issue," Butler said.

These laws, designed to prevent ID theft, are often modeled on California's law, Butler noted. Under §1798.81.5 of the California Code, businesses that own or license personal information about California residents must implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.[2] When a security breach does occur, the business must notify any resident whose information was, or was reasonably believed to have been, acquired by an unauthorized person. The law further states that residents should be notified "in the most expedient time possible and without unreasonable delay. . ."[3]

Laws addressing security breaches are expected to spread to more states in light of a recent theft at Providence Home Services, an Oregon-based provider, where storage tapes containing 365,000 patient records were stolen from an employee's car, said Butler. According to the Washington Attorney General's Office, the stolen data contained patients' names, addresses and birthdates, as well as the Social Security numbers of approximately 250,000 patients.

In another example, the defendant in *United States v. Ramirez*, pled guilty of violating the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rules after she sold confidential medical record information belonging to a special agent with the Federal Bureau of Investigation (FBI).[4] The woman knowingly sold the information to a person she believed was working for a drug trafficker, according to a statement by U.S. Attorney for the Southern District of Texas,

Chuck Rosenberg. The government proved that during the spring of 2005, the woman was employed at a doctor's office that was under contract to provide physical examinations and medical treatment to FBI agents, Rosenberg said. For $500, she offered and agreed to provide the FBI agent's personal and medical information to an individual she thought was working for a drug trafficker. The person was a confidential FBI source who recorded their various meetings.

The woman was charged with using and causing to be used a unique health identifier, with the intent to sell, transfer, and use it for personal gain and malicious harm. She faces a maximum 10-year prison term without parole and a $250,000 fine.

Federal security breach notification and security law. The issue of security breaches has not gone unnoticed at the federal level either. Several different congressional committees in both the House and Senate have focused their attentions on beefing up security laws. In a November 7, 2005, letter to Congress, the National Association of Attorneys General (NAAG) applauded the federal efforts at enacting a national law and highlighted the advances already made at the state level. The letter called on Congress to enact a security breach notification law that would provide meaningful information to consumers. "If Congress is not able to enact a strong notice law, it should leave the issue to state law, which is responding strongly."

The letter, which was signed by 48 attorneys general, stressed that a national law should be at least as protective as the law in California. In particular, the NAAG letter stressed that the standard for notification should be tied to whether personal information, in either electronic or paper form, was believed to have been acquired or accessed by an unauthorized person, rather than a standard that includes an additional requirement that the breach entail actual harm or a measure of risk of harm. According to NAAG, at the time of the letter the majority of states with security breach notification laws – California, Georgia, Illinois, Indiana, Maine, Minnesota, Nevada, New York, North Dakota, Ohio, Rhode Island, Tennessee, and Texas – did not require any additional trigger, such as actual harm, before notice about a breach must be given to affected customers.

The letter also called on Congress to preserve the right of the states to address security breach issues should a national law be enacted. According to NAAG, state attorneys general should be able to enforce any national security breach law. In addition, NAAG urged Congress to avoid preempting state security breach laws. The letter stressed that "[T]he states have been able to respond more quickly to concerns about privacy and identity theft involving personal information, and have enacted laws in these areas years before the federal government."

Recommendations for organizations. Organizations should establish policies and procedures, form a response team, and encrypt or even remove sensitive information from records, Butler said. He stressed that "the more an organization can do before a breach occurs to facilitate a rapid response, the better shape it will be in when an event does happen."

Butler said that to prevent a breach and mitigate the affects if one occurs, organizations should:

- Determine what information in the system might trigger a notification requirement, such as names and SSNs. "If they are utilizing records with those two pieces of information on them, they should do a new record inventory and find out where that information is."
- Put together an instant response team. The team should consist of information technology (IT), legal, and communications personnel, as well as human resources personnel if the theft or loss involves employee data.
- Create policies and procedures for responding to a breach.
- Create a template notification form. The document could be modified depending on the type of breach. Butler recommended developing a uniform notification that follows the strictest state laws for those affected.
- Minimize the chance of exposure by encrypting information and migrating away from SSNs.
- Comply with the HIPAA Security Rule requirements, such as developing a disaster recovery plan and backing up information.

Final notes. Responses to security breaches will vary depending on the facts, said Butler. For example, some states such as California allow substitute notice (such as posting on a website and sending via e-mail) if the cost of written notification would exceed certain thresholds.

Butler emphasized, however, that organizations should follow the strictest state laws when personal information from residents in several states has been stolen. "At the end of the day, how you respond may have a lot more to do with establishing or maintaining the trust of your customers or clients and patients rather than just satisfying the bare minimum of what a particular law may require," he concluded.

CCH Washington Bureau, April 5, 2006.

[1] "MEDICAL IDENTITY THEFT: The Information Crime That Can Kill You," Pam Dixon, Executive Director, World Privacy Forum, May 3, 2006. The full text of this report is located at www.Worldprivacyforum.org/medicaidentitytheft.html.

[2] CIV. §1798.81.5.

[3] CIV. §1798.82.

[4] *United States v. Ramirez,* No. 7:05-CR-00708, S.D. Tex., March 6, 2006.

crowell moring

STATE LAWS GOVERNING SECURITY BREACH NOTIFICATION

www.crowell.com

State	Laws & Effective Dates	Trigger - Information Materially Compromised or Likelihood of Harm Before Notification Required?	Exemptions	Pre-Breach Measures Required
Arizona	SB 1338, Effective 1/1/07	Yes	GLB & HIPAA, One that follows notification procedures or security breach policy of primary or functional federal regulator is deemed compliant.	No
Arkansas	SB 1167, Effective 8/12/05	Yes	Entities covered by any state or federal regulations offering greater protection or equal disclosure requirements are exempt.	Yes
California	SB 1386, Effective 7/1/03	No	Entities covered by state medical, financial and vehicle confidentiality codes and HIPAA are exempt from pre-breach measures, but not notification requirements.	Yes
Colorado	HB 1119, Effective 9/1/06	Yes	Partial exemption for GLB, An entity is deemed compliant if it maintains procedures for breach of security pursuant to mandate by primary or functional regulator.	No
Connecticut	SB 650, Effective 1/1/06	Yes	An entity is deemed compliant if it maintains a security breach procedure under GLB and notification is given in event of breach.	No
Delaware	HB 116, Effective 6/28/05	Yes	Entities regulated by state or federal law with greater protection of personal information than is provided by this chapter are deemed compliant.	No
Florida	HB 481, Effective 7/1/05	Yes	An entity is deemed compliant if the entity has a notification procedure pursuant to federal regulations and follows it. Government agencies exempt from fines.	No
Georgia	SB 230, Effective 5/5/05	No		No
Idaho	SB 1374, Effective 7/1/06	Yes	An entity is deemed compliant if the entity maintains procedures for breach of security pursuant to mandate by its primary or functional regulator.	
Illinois	HB 1633, Effective 1/1/06	No		No
Indiana	HB 1101, Effective 7/1/06	No	A data base owner is not required to make disclosure under this chapter if it maintains its own disclosure procedure that is as stringent as this chapter, or is required to make disclosure under a federal statute, regulation or guideline.	Yes
Kansas	SB 196, Effective 7/1/06	Yes	If an entity is regulated by state or federal regulators and maintains a procedure for breach of security, it is deemed compliant.	Yes
Louisiana	SB 205, Effective 1/1/06 [or when rules promulgated by AG]	Yes	Financial institutions subject to Interagency Guidelines on security breach and notice requirements are deemed compliant with this law.	No
Maine	LD 1671, Effective 1/31/06	No		No
Minnesota	HF 2121, Effective 1/1/06	No	Entities covered by GLB and HIPAA are exempt.	No
Montana	HB 732, Effective 3/1/06	Yes		Yes
Nebraska	LB 876, Effective 4/7/06	Yes	An entity is deemed compliant if it is regulated by state or federal regulators and maintains procedures for a breach in security and if it notifies in the event of a breach.	No
Nevada	SB 347, Effective 1/1/06 [10/1/08 for mandatory encryption]	Yes	Entity which is subject to and complies with GLB privacy and security provisions shall be deemed compliant with notification provisions of the Nevada statute. Some entities exempt from pre-breach requirements.	Yes
New Jersey	A4001, Effective 1/1/06	Yes		Yes
New York	S 3492 & S 5827, Effective 12/7/05	No		No
North Carolina	SB 1048, Effective 12/1/05	Yes	Pre-breach measures are not applicable to entities subject to GLB, HIPAA, and FCRA. Financial institutions subject to federal Interagency Guidelines on security breach and notice requirements are deemed compliant.	Yes
North Dakota	SB 2251, Effective 6/1/05	No	Financial institutions subject to Interagency Guidelines on security breach and notice are deemed compliant with this law.	No
Ohio	HB 104, Effective 2/17/06	Yes	Financial institutions already subject to federal notification requirements are deemed compliant. The law does not apply to those regulated by the HIPAA provisions of the Social Security Act.	No
Pennsylvania	SB 712, Effective 6/20/06	Yes	A financial institution that complies with the notification requirements of the Interagency Guidelines is deemed compliant, and any entity that complies with the notification requirements of its primary or functional federal regulator shall be in compliance with this act.	No
Rhode Island	HB 6191, Effective 3/1/06	Yes	Any person who maintains security breach procedures pursuant to rules of its primary or functional regulator is deemed compliant with notification requirements. Financial institutions governed by the Interagency Guidelines, and health care entities governed by HIPAA are deemed compliant with the chapter.	Yes
Tennessee	HB 2170, Effective 7/1/05	Yes	Entities covered by GLB are exempt.	No
Texas	SB 122, Effective 9/1/05	No	Financial institutions as defined by 15 USC 6809 are exempt from the pre-breach duties.	Yes
Utah	SB 69, Effective date 1/1/07	Yes	Entities regulated under state or federal law that maintain a procedure for breach of security and notify in the event of breach.	Yes
Washington	SB 6043, Effective 7/24/05	Yes		No
Wisconsin	SB 164, Effective 3/30/06	No		No

Updated 5/23/06

CMS proposes rule for DME competitive acquisition programs

by Michelle Oxman, J.D., Contributing Editor

CMS has issued a proposed rule to phase in the competitive acquisition program (CAP) for durable medical equipment, prosthetics, orthotics and supplies (DMEPOS) under Medicare Part B. After CMS authorized a series of demonstration projects testing a CAP, the Medicare Modernization Act (MMA) (PubLNo. 108-173), §302(b) required CMS to move from the use of fee schedules to competitively bid contracts for DMEPOS.

The proposed rule begins the implementation of CAP for certain items of durable medical equipment (DME) and enteral nutrition, their associated supplies, and off-the-shelf orthotics. The proposed rule also implements changes to Medicare payments for oxygen equipment and certain rented DME enacted in the Deficit Reduction Act of 2005 (PubLNo. 109-171).

Prevention of fraud and abuse. In addition to saving money for both the government and beneficiaries, an important purpose of the CAP is the prevention of fraud and abuse. Even with the implementation of the enrollment standards at 42 C.F.R. §424.57, CMS believes there has not been sufficient oversight of suppliers of DMEPOS and other items related to the quality and provision of their products. The Office of Inspector General (OIG) has conducted several investigations of suppliers of DMEPOS and other items to determine the legitimacy of their businesses and has uncovered many examples of fraud and abuse including:

- billing for services not performed;
- billing for a more expensive service than was rendered;
- billing separately for several services that should be combined into one billing;
- billing twice for the same service;
- billing for more expensive equipment or supplies than were used;
- offering or receiving kickbacks (that is, offering or accepting something in return for services);
- offering or accepting a bribe to use a particular service or company;
- providing unnecessary services; and
- submitting false cost reports.

Initial implementation. Areas that may be exempt from competitive acquisition of DMEPOS include rural areas and areas with low population density within urban areas that are not competitive, unless there is a significant national market through mail order for a particular item or service.

CMS has discretion under the law to first phase in DMEPOS items for bidding based on high cost and volume or largest savings potential. Suppliers in a competitive bidding area (CBA) would submit bids for selected items, and CMS would use these bids to establish Medicare payment amounts for these items. Under the proposed rule, the Medicare payment amounts would be the median of the winning suppliers' bids for selected items. Suppliers whose bids are lower than the Medicare payment amounts set under the competitive bidding program could offer a rebate to beneficiaries, lowering their costs for acquiring the DME items they need.

When competitive bidding is implemented, beneficiaries who live in a CBA will be permitted to obtain DMEPOS only from contracted suppliers. Beneficiaries whose permanent residence is outside a CBA but visit a CBA also will be required to obtain their DMEPOS from contracted suppliers because of CMS' policy to direct new business only to contracted suppliers.

The CAP will be phased in over several years. CMS proposed to implement the program in 10 of the largest metropolitan areas in 2007, 80 more cities in 2009, and others after 2009. The Metropolitan Statistical Areas (MSAs) of New York City, New York; Chicago, Illinois and Los Angeles, California are excluded from the 2007 group. Any MSA that crosses the boundaries of DME regional carriers (DMERCs) also will be excluded. CMS expects to implement competitive bidding in these areas in 2009.

Special rules for particular categories of DMEPOS. Oxygen supplies must be paid at a monthly rate with an add-on for portable equipment. Rental items that do not require substantial maintenance and servicing usually are inexpensive, with payment limited to the approximate purchase price. The proposed rule provides for "grandfathering" in suppliers of certain rented DME items and oxygen supplies with whom arrangements existed before the start of the competitive bidding program.

Elements of the CAP. The major features of the CAP include:

(1) establishment of quality standards to be required of DMEPOS providers and suppliers according to the particular items each provides or supplies;
(2) establishment of a program advisory and oversight committee to advise the Secretary on the quality standards, financial standards, data collection, best practices and other aspects of the program;
(3) designation of national accreditation organizations with deeming authority to evaluate and confirm compliance with the standards;
(4) a requirement that bidders be accredited either by the applicable state agency or by an accreditation organization with deeming authority;
(5) designation of CBAs which will be served by the contracted DMEPOS providers and suppliers;
(6) establishment of prices for items by state or CBA;
(7) increased oversight to prevent and detect fraud and abuse; and
(8) clarification and enforcement of the exclusion of low vision aids such as magnifiers from Medicare coverage under the exclusion of eyeglasses.

The proposed rule was published in the May 1 *Federal Register (see Health Care Compliance Letter, ¶730,008).* ■

CMS Release, April 24, 2006.

HIPAA

Physician lacked right to request injunction under HIPAA

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

A physician did not have the right under the Health Insurance Portability and Accountability Act of 1996 (PubLNo. 104-191) (HIPAA) to request a federal injunction against a medical insurance carrier to prevent it from reporting an adverse action to the Health Care Integrity Protection Data Bank (HIPDB), according to the U.S. District Court for the District of Tennessee.

Petition for temporary injunction. The carrier advised the physician that it would revoke his credentials and terminate all provider contracts in accordance with the carrier's corrective action plan. The carrier claimed that under regulations promulgated under HIPAA, the giving of such notice triggered an obligation to report its adverse action to the HIPDB. The physician filed a petition for temporary injunction requesting that the carrier be prohibited from terminating the agreement or reporting any adverse action until the appeals process was exhausted.

Administrative mechanism for disputes. HIPAA, however, does not provide a private right of action. In addition, the HIPAA regulations provide for a comprehensive administrative mechanism for a practitioner to dispute the accuracy of a report of an adverse action entered into the HIPDB. The court compared HIPAA regulations with Health Care Quality Improvement Act of 1986 (HCQIA) regulations, which were passed to benefit patients by improving the quality of health care and reducing the number of incompetent physicians. Accordingly, the court denied the petition for temporary injunction to the extent that it sought relief related to the carrier's HIPDB reporting requirements.

The dispute regarding the proper interpretation of the physician participation agreement and other contractual relationships between the physician and carrier were predominately matters of state law and, therefore, were remanded to state court. ■

Carter v. BlueCross BlueShield of Tennessee, Inc., E.D. Tenn., April 24, 2006, Health Care Compliance Reporter, ¶800,136.

In the News

Tenent, OIG reach agreement to avoid exclusion

In response to the OIG's announcement that it intended to exclude Alvarado Medical Center from participation in the federal health care programs, Tenent Healthcare Corp., Alvarado's parent corporation, has agreed to close or transfer ownership of Alvarado. On May 8, 2006, the OIG notified Tenent of the intent to propose exclusion based on Alvarado's alleged payments of kickbacks to physicians. Alvarado was charged with funneling $10 million in kickbacks to referring physicians between 1992 and 2002 through physician relocation agreements; however, both the government's attempts at prosecution ended in mistrial.

OIG Press Release, May 17, 2006.

Mental health facility civil rights violations identified

The Department of Justice (DoJ) announced that it has reached a settlement with the State of California regarding civil rights violations at four state mental hospitals providing care to individuals who were either committed civilly or through criminal proceedings. The DoJ investigation revealed significant civil rights violations including a pattern of preventable suicides and serious, life threatening assaults on patients by staff and other patients. The investigation was conducted pursuant to the Civil Rights of Institutionalized Persons Act (CRIPA), which allows the federal government to identify and root out systemic abuses rather than focus on individual abuses.

DoJ Press Release, May 2, 2006.

Reminder of available funds for treatment to undocumented aliens

A Medicare Learning Network Special Edition article was released by CMS to inform and remind providers of available funding for emergency health services furnished to undocumented aliens. The section 1011 of the Medicare Modernization Act of 2003 provides $250 million each year for fiscal years 2005-2008 for payment to eligible providers of such services. Two-thirds of the funds are divided among all 50 states and the District of Columbia, based on their relative percentages of undocumented aliens, and one-third of the funds are divided among the six-states with the largest number of undocumented alien apprehensions. As of May 1, 2006, over 9,000 provider applications have been approved. The first section 1011 payment to providers was issued on February 27, 2006, totaling nearly $25 million. The next quarterly payment will be made on May 29, 2006.

MLN Matters, SE0633, May, 2006.

Two Texas DME fraud schemes detected

In unrelated schemes, a Texas physician and Texas durable medical equipment (DME) company operator were sentenced to 10 years and 30 months respectively for committing fraud in connection with selling durable medical equipment. The physician and her office manager sold fraudulent certificates of medical necessity and prescriptions for motorized wheelchairs and other DME. The DME company operator fraudulently billed Medicare and Medicaid for power wheelchairs and other equipment that was not provided or prescribed by a doctor. The physician was ordered to pay $13 million in restitution, and the DME company operator was ordered to pay $253,000.

OIG Press Release, April 2006.