CCH Healthcare Compliance LETTER

Volume 5, Issue 20 www.cchgroup.com October 14, 2002

Letters to the Editor

The CCH Healthcare Compliance team welcomes comments regarding articles published in the CCH Healthcare Compliance Letter. Send comments to Jeff Reinholtz, Managing Editor at reinholj@cch.com. Comments may be edited for clarity or space.

For more information about the CCH Healthcare Compliance Portfolio visit our online store at **http://health.cch.com.**

Pharmaceutical industry gets draft Guidance from OIG

by Geraldine S. Stroka J.D., R.N.

The Office of Inspector General (OIG) determined that the main risk areas for pharmaceutical manufacturers are issues relating to the integrity of the data used to establish payment, kickbacks and other illegal remuneration, and compliance with laws regulating drug samples. These areas were included in the much-anticipated Draft Compliance Guidance for Pharmaceutical Manufacturers issued by OIG on September 30, 2002.

On that same day, Janet Rehnquist, the Inspector General for the Department of Health and Human Services (HHS), announced the Guidance during her address at a joint meeting of the American Health Lawyers Association (AHLA) and the Health Care Compliance Association (HCCA) in Washington, D.C. She also unveiled plans for a combined (OIG, AHLA, and HCCA) effort in developing a pamphlet to assist boards of directors in promoting compliance within their corporations.

Drug pricing and anti-kickback issues. Rehnquist stated that because pharmaceutical companies report data used by federal and state healthcare programs in establishing reimbursement rates, the pharmaceutical companies themselves are responsible for the integrity of this data. Depending on the specific circumstances, if the information supplied is inaccurate or false, the False Claims Act, civil money penalties or the Anti-Kickback Statute could be triggered. Manufacturers' prices must accurately reflect rebates, discounts, coupons, or similar benefits.

Potential risk areas under the Anti-Kickback Statute could arise from pharmaceutical manufacturers' relationships with purchasers, physicians and other healthcare professionals, as well as sales agents. The risk occurs because the relationship could provide prohibited inducements that ultimately impact the Medicare or Medicaid healthcare programs. If the purpose of such a relationship is to create an inducement and the arrangement is not protected under a safe harbor provision, an anti-kickback violation may occur.

Emphasizing that the government has, in the past, paid far too much for medications, Rehnquist faulted several drug-pricing methods, the Average Wholesale Price (AWP) and the "spread." She stated the AWP, a drug reimbursement methodology for prescription drugs under Medicare Part B, was "flawed," because it may not represent the actual price paid. In addition, she stated that the "spread," the difference between the cost of the medication to the physician and the amount that government programs paid for the medication, might be used as a marketing tool to lure physicians. Rehnquist clarified that although pharmaceutical manufacturers do not directly bill the government for medications, they directly influence the spread. Anti-kickback issues arise when there is evidence that drug prices are manipulated to induce someone to purchase them and there is active marketing of the "spread."

Also, pharmaceutical manufacturers need to review their relationships with physicians and their own sales staffs. At a minimum, all dealings with physicians should follow the Pharmaceutical Code on Interactions with Healthcare Professionals (PhRMA Code), a voluntary code effective July 1, 2002. This Code was enacted by the Executive Committee of the Pharmaceutical Research and Manufacturers of America, and is available on its Website at http://www.phrma.org. In addition, manufacturers' must review their sales force arrangements to determine if their compensation programs fit the safe harbor for personal services arrangements and employment. Such manufacturers should also develop comprehensive training programs for these sales staffs.

Drug samples. Manufacturers need to comply with the Prescription Drug Marketing Act of 1987 (PDMA) which governs the distribution and sale of prescription drugs or face sanctions under the Act. Rehnquist stated, "Free is free;" if it is free to a patient, it is free to the government.

Board of directors' compliance tool. Rehnquist announced that the OIG, AHLA, and HCCA would develop an educational pamphlet for healthcare companies' boards of directors. This pamphlet would contain questions directors need to ask compliance officers of the healthcare companies on whose board they serve. ■

Draft OIG Compliance Program Guidance for Pharmaceutical Manufacturers, 67 FR 62057, Oct. 3, 2002, ¶151, 018

Safe harbor provisions for waivers of coinsurance and deductibles expanded

by Raio G. Krishnayya, J.D.

The Office of Inspector General (OIG) has issued a proposed rule to expand the safe harbors provided under the Anti-Kickback Statute (42 U.S.C. §1320a-7b(b)). The proposed rule would grant safe harbor status to waivers of coinsurance and deductible under the Medicare SELECT program for beneficiaries under Medicare Part A or B programs. Specifically, the proposed safe harbor is designed to expand the protection already granted to Medicare SELECT policyholders. Currently, only Medicare SELECT waivers for coinsurance or deductibles that pertain to inpatient hospital treatment are afforded safe harbor protection. The proposed rule would allow broader protection for waivers associated with Part B cost-sharing initiatives (i.e. beyond the inpatient hospital waiver programs).

Medicare SELECT waiver programs must adhere to the guidelines for acceptable waivers issued by the Centers for Medicare and Medicaid Services (CMS).

The OIG listed several factors that prompted expansion of the safe harbor provisions. For example, a study had been conducted to determine how the absence of a safe harbor could affect expansion of the Medicare SELECT networks beyond hospitals. The result demonstrated that the absence of such a safe harbor would severely hinder such expansion.

Another factor was that congressional intent in establishing the Medicare SELECT program was to expand the SELECT program to give beneficiaries wider latitude in choosing supplemental insurance. However, the current safe harbor provisions regarding the Medicare SELECT program have stifled such expansion.

In addition, reimbursement trends have made significant changes. The trend demonstrates that providers are attempting to move away from cost-based and charge-based reimbursement programs to prospective payment programs.

OIG has issued a caveat regarding the expansion of this proposed safe harbor. Medicare SELECT waiver programs must adhere to the guidelines for acceptable waivers issued by the Centers for Medicare and Medicaid Services (CMS). The OIG predicted that charges based on a fee-for-service reimbursement method would probably not be subject to an authorized waiver. Thus, under this proposed safe harbor, CMS would maintain exclusive control of the Medicare SELECT program.

Comments regarding this proposed safe harbor must be received by 5 p.m. on October 25, 2002. ■

Proposed Rule, 67 FR 60202, Sept. 25, 2002, ¶100,916

CCH Healthcare Compliance Letter

Managing Editor
Jeff Reinholtz, J.D.

Coordinating Editors
Raio G. Krishnayya, J.D.
Gordon R. Shea, J.D.
Geraldine S. Stroka, J.D., R.N.
Judith A. Tichenor, J.D., LCSW

CCH Washington Bureau
HHS, CMS–Brendan Frost
DOJ, FTC–Peter Feltman
Capitol Hill–Catherine Hubbard, Jeff Carlson
White House–Paula Cruickshank

Developmental Editors
Patrick J. Osborne
Sharon Sofinski

Designer
Don Torres

Comments from readers are welcome and should be directed to Jeff Reinholtz at REINHOLJ@CCH.COM, Tel. 847-267-7316, 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.

Proposed Health Records Confidentiality Act targets marketers

by Gordon R. Shea, J.D.

While congressional critics have spent months threatening to undo the Bush administration's changes to the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA), one of the first actual steps in that direction has now been taken: specific legislation has been proposed to undo the Privacy Rule's marketing provisions.

The proposed legislation, titled the Health Records Confidentiality Act of 2002, was drafted by Sen. Bill Nelson (D-Florida) in late August. It aims to close what Nelson and other advocates of strong medical privacy protections call a marketing "loophole" in HIPAA's recently-finalized Privacy Rule —a loophole that Nelson says "lets drug companies and pharmacies mine and secretly profit from" patients' "most private medical information."

Pharmaceutical focus. The Nelson proposal targets marketing efforts by pharmaceutical companies. Under Nelson's legislative language, healthcare providers and others that wished to supply pharmaceutical companies information for marketing purposes would first need to obtain patients' written consent. The proposal would exempt any communications that are "made as part of the treatment of a patient" from the definition of marketing when such communications are "for the purpose of furthering" medical treatment.

The proposal would require pharmaceutical marketers to provide "clear and conspicuous notice" to patients of the marketers' disclosure practices, and would force marketers to obtain written patient consent to each disclosure. It would also return the focus of the Privacy Rule's marketing provisions to where it had been under previous versions of the Rule: the *purposes* of suspect communications.

Hybrid return? In some ways, the proposals represent a hybrid of ideas that were part of the Privacy Rule before the Bush administration's Department of Health and Human Services (HHS) changed the Rule earlier this year (albeit a hybrid limited to pharmaceutical companies). Under an earlier version of the Privacy Rule favored by many Democrats, "marketing" was defined as any communication that, as one of its purposes, encouraged recipients to use or purchase certain products or services. Other language in the old version of the Rule would have required marketers to inform recipients of sales-type communications as to how the recipients could stop receiving the communications. More generally, this earlier version of the Privacy Rule was built around the idea of consent: healthcare patients could not be subjected to unwanted marketing or disclosures of their private health information unless they consented beforehand, usually in writing.

Earlier this year, however, the Bush HHS department changed all of this. Among other alterations, HHS redefined the word "marketing" as it was used in the law and eliminated language that would have allowed patients to opt out of receiving marketing-related communications. As finalized this August, the Bush version of the Privacy Rule no longer focuses on the purposes of marketing-related communications. The finalized Bush Privacy Rule also exempts three particular classes of communications from its definition of marketing, and eliminates both the law's opt-out provisions and its consent-based principle.

Florida at the fore. Nelson's state of Florida has been the setting for a number of recent problematic marketing schemes involving pharmaceutical companies. For example, pharmaceutical company Eli Lilly was recently investigated by Florida's attorney general after it mailed unsolicited samples of the anti-depressant drug Prozac to at least two state residents. In another matter, pharmaceutical retailer Eckerd recently settled accusations that it buried marketing authorizations within the fine print of forms that customers were required to complete before they picked up prescriptions.

Links to Sen. Nelson's recent statements on medical privacy and to the text of his proposed legislative language addressing the pharmaceutical marketing "loophole" of HIPAA are available at http://billnelson.senate.gov/newpages/medicalpriv.cfm#. ■

CCH Chicago Bureau, Oct. 3, 2002

On The Front Lines

You can't have privacy without security

by Paris Cavic, J.D., MBA

With the finalization of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, a vital component of privacy–maintaining privacy by securing the information–may have been given short shrift. However, prudent organizations have recognized and will continue to recognize that privacy cannot be achieved while security is left in a vacuum, and therefore will begin to take steps using the principles in the proposed security rule as guidance for securing their electronically maintained individually identifiable health information.

The Department of Health and Human Services (HHS) published a proposed rule for Security and Electronic Signature Standards ("Security Standards") on August 12, 1998, more than four years ago. While this may seem like a millennium ago in the information technology field, the basic security standards spelled out in the proposed rule offer significant guidance for those covered entities seeking to secure their private, individually identifiable health information. Confidentiality is threatened not only by the risk of improper access to electronically stored information, but also by the risk of interception during electronic transmission of the information.

In the proposed Security Standards, HHS proposes standards for electronically maintained health information. The proposed rule would mandate that health plans, healthcare clearinghouses, and healthcare providers have Security Standards in place to comply with the statutory requirement that healthcare information and individually identifiable healthcare information be protected to ensure privacy and confidentiality when such information is electronically stored, maintained, or transmitted.

The security provisions of Section 262 of HIPAA applies to any health plan, any healthcare clearinghouse, and any healthcare provider that electronically maintains or transmits any health information relating to an individual.

Section 142.308 of the proposed rule would set forth the security standard. HHS has recognized that there is no single standard that integrates all the components of security (administrative procedures, physical safeguards, technical security services, and technical mechanisms) that must be in place to preserve health information confidentiality and privacy as defined in the law. Therefore, HHS has proposed designating a new, comprehensive standard, which defines the security requirements to be fulfilled. The high-level concepts that HHS has based on the Security Standard are:

- The Security Standard must be comprehensive. Specifically, if a system or communications between two systems were implemented with technology meeting standards in a general system security framework (identification and authentication; authorization and access control; accountability; integrity and availability; security of communication; and security administration), that system would be essentially secure.
- The Security Standard must be "technologically neutral." HHS recognizes that technology is changing quickly, and wants to factor in the flexibility for future advances in security technology.
- The Security Standard would need to be scalable from the smallest provider to the largest affected entities commensurate with the operations and risks faced by the covered entities, and the economic realities associated with safeguarding individually identifiable health information.

Implementation Requirements

The Security Standard does not address the extent to which a particular entity should implement specific features. Instead, HHS would require that each affected entity assess its own security needs and risks and devise, implement, and maintain appropriate security to address its business requirements. How individual security requirements would be satisfied and which technology to use would be business decisions that each covered entity would have to make.

As a result of HHS's collaborative Security Standard development process, implementation of the proposed Security Standards, for purposes of presentation only, fall into the following four categories:

Administrative procedures to guard data integrity, confidentiality, and availability. These are documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data. Features for the administrative procedures category that would be required and are further detailed in the implementation requirements of the proposed Security Standard are certification of security compliance, chain of trust partner agreement, contingency plan, formal mechanism for processing records, information access control, internal audit, personnel security, security configuration management, security incident proce-

dures, security management process, and termination and training of personnel.

Physical safeguards to guard data integrity, confidentiality, and availability. These are standards that relate to the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Physical safeguards also cover the use of locks, keys, and administrative measures used to control access to computer systems and facilities. Features for the physical safeguards category that would be required and are further detailed in the implementation requirements of the proposed Security Standard are assigned security responsibility, media controls, physical access controls, policy/guidelines on workstation use, secure workstation location, and security awareness training.

Technical security services to guard data integrity, confidentiality, and availability. These include the processes that are put in place to protect and to control and monitor information access. Features for the technical security services safeguards category that would be required and are further detailed in the implementation requirements of the proposed Security Standard are access control (procedure for emergency access would be required to be implemented; in addition, at least one of the following three implementation features must be implemented: context-based access, roll-based access, or user-based access), audit controls, authorization, data authentication, and entity authentication (the following features would be required to be implemented: automatic logoff, unique user identification, and at least one of the other listed implementation features).

Technical security mechanisms. These include the processes that are put in place to prevent unauthorized access to data that is transmitted over a communications network. Features for the technical security services safeguards category that would be required and are further detailed in the implementation requirements of the proposed Security Standard are communications/network controls. The following implementation features would be required to be implemented: integrity controls and message authentication. If communications or networking is employed, one of the following implementation features would also be required to be implemented: access controls or encryption. In addition, if using a network, the following four implementation features would be required to be implemented: alarm, audit trail, entity authentication, and event reporting.

In the proposed Security Standards, the administrative requirements, physical safeguards, technical security services, and technical security mechanisms and supporting implementation features are presented at proposed §142.308(a) through §142.308(d). HHS would require each to be documented, would require the documentation to be made available to those individuals responsible for implementing the procedures, and would require it to be reviewed and updated periodically. The matrix presented at 63 Fed. Reg. 43269 depicts the requirements and supporting implementation features for each component of the proposed Security Standards.

Integrating Security into Privacy

Taking into consideration HHS's position that the Security Standards were developed to be comprehensive and technology neutral, covered entities should begin to incorporate reasonable security for the protection of personally identifiable health information. Security requirements, whether they incorporate the proposed Security Standards or current information technology standards, should be included in the Privacy Compliance Program.

Furthermore, the Privacy Rule offers guidance for the implementation of security measures at 45 CFR §164.530(c), which requires a covered entity to have in place appropriate technical, administrative, and physical safeguards for the protection of individually identifiable health information.

Covered entities should, at a minimum, incorporate, develop, and document the following in establishing security standards for their organization:

Organizational risk assessment. The proposed Security Standard requires that each healthcare entity engaged in electronic maintenance or transmission of health information assess potential risks and vulnerabilities to the individual health data in its possession in electronic form.

Build security compliance infrastructure. This would include the assignment of responsibility for overseeing security within the covered entity, and the development of entity specific representation within the security oversight infrastructure, including representation from end users.

Develop policies and procedures. Policies and procedures should be developed that define and document not only the security requirements, but also the standards and responsibility for maintaining the security program.

Implement reporting mechanisms. This would include reporting of security violations as well as reporting to the highest levels of the organization.

Training. All employees should be indoctrinated, and regularly refreshed, in the requirements of the security program and their responsibilities in regard to maintaining the security of individually identifiable health information.

Develop and implement auditing and monitoring. Covered entities should utilize a regular audit of their internal security policies and procedures as well as utilize the audit controls and mechanisms found in software.

The degree of development and documentation will have to be scaled to the size of the organization and the risks identified within the security assessment. HHS recognizes that the size and scope of a security program will differ from covered entity to covered entity.

Paris Cavic, JD, MBA, is the President of the Healthcare Compliance Group, LLC, and a practicing attorney. Prior to forming the Healthcare Compliance Group, LLC, Mr. Cavic worked with and for physicians, hospitals, and HMOs in many areas of corporate compliance as a consultant and attorney. He may be reached at parisesq@usa.net.

Chandler and *Dunleavy* could eliminate entire class of FCA defendants

by Raio G. Krishnayya, J.D.

Although more than 100 years old, the False Claims Act (FCA) has proven to be a continuously changing legal landscape. The next term for the U.S. Supreme Court will be proof of the FCA's dynamic nature, when it hears the case on appeal from the U.S. Court of Appeals for the Seventh Circuit, *United States ex rel. Chandler v. Cook County*. As previously reported in Vol. 5, Issue 4 of the CCH Healthcare Compliance Letter, two cases have emerged that have resulted in a divide among federal circuits, of whether counties are "persons" and therefore, within the purview of the FCA's reach.

United States ex rel. Chandler v. Cook County, the case heard by the Seventh Circuit, held that counties were "persons" under the FCA and thus, not entitled to protection under the doctrine of sovereign immunity. The result of Seventh Circuit's decision prompted Cook County to file its request for U.S. Supreme Court review. In June, the U.S. Supreme Court granted that request for review; however, oral argument has not yet been scheduled.

The other case, *United States ex rel. Dunleavy v. County of Delaware,* was heard by the U.S. Court of Appeals for the Third Circuit. The outcome of that case was exactly opposite of the *Chandler* case. In May, Anthony Dunleavy filed his request for Supreme Court review, however, the Court has neither granted nor denied this request.

Broad importance. The Supreme Court's decision with regard to the *Chandler* case will carry broad FCA implications because their decision could effectively eliminate an entire class of potential defendants from FCA liability. In the healthcare arena these decisions directly affect hospitals that are run by the county government. Consider that according to a 1997 health care survey conducted by the U.S. Census Bureau, there are 1,591 government-run hospitals in the United States. Thus, depending on the Supreme Court's interpretation of the term "person" many of those hospitals could be completely immune from FCA liability.

Indications. The *Chandler* case will be argued against the backdrop of the *Vermont Agency of Natural Resources v. United States ex rel. Stevens* case (*See* CCH ¶300,153). *Vermont Agency of Natural Resources* is about a former employee of a Vermont-state entity, who filed a FCA claim against his former employer for allegedly false claims submitted to the U.S. Environmental Protection Agency for reimbursement under federal programs. Facing the Supreme Court, was whether a state agency was a "person" as contemplated by the drafters of the FCA. Additionally, had the Court found that a state agency was a person then the Court would have had to determine whether the doctrine of Sovereign Immunity protected a state agency from FCA liability.

The Court never reached the merits of whether the Sovereign Immunity doctrine applied because the preliminary question was answered in the negative; the term "person" was not intended to include state agencies within its purview. The Court cited three reasons for their conclusion. First, the Court looked at the language throughout the FCA. In one section of the FCA, there is express inclusion of states (31 U.S.C § 3733 or the Civil Investigation Demand (CID) provision). In the *qui tam* provision, however, such express language was absent. Therefore, the Court concluded that if Congress had intended states to be part of the *qui tam* provision or to be subject to punitive damages under the FCA, Congress would have included such language. Second and historically, punitive damages generally may not be levied against governmental entities. Third, a comparison of similar statutes like the Program Fraud Civil Remedies Act of 1986 also indicates an absence of language expressly holding state entities liable. Furthermore, the Court noted that in such circumstances, courts have not held state entities liable where there is no actual language of inclusion. This last point is the extension of the first point.

In support of their positions, the county entities in *Chandler* and *Dunleavy* would probably assert the rationale of *Stevens*. However, their positions may not be as strong as the State of Vermont in *Stevens* because they would have to show that municipalities and counties are simply extensions of the state and thus, subject to constitutional protection of their sovereignty, just as the states are. While this argument may be a stretch, there is legal support as cited in the *Dunleavy* petition for writ of certiorari (the formal request for Supreme Court review).

The case cited in the petition and relied upon by municipalities and counties to avoid being named in a FCA suit is a U.S. Court of Appeals for the Fifth Circuit case, *United States ex rel. Garibaldi v. Orleans Parish School Board*. The case invoked a "city immunity" doctrine, which protected municipalities from the punitive damages clause. The rationale adopted by the Fifth Circuit is similar to that used in the *Stevens* case in that punishing municipal tax payers (i.e. the costs associated with punitive damages would be spread among the tax payers in the form of higher taxes) would be unjust.

The *Garibaldi* case is a strong case for the county entities to cite for the primary reason that it does not try to assume that counties or municipalities are simply extensions of state entities (although it would help their case if they could show that link). Instead, that case takes the reasons that the Supreme Court has articulated for protecting state entities and asserts that the same reasons apply to protecting counties and municipalities from the FCA vis-à-vis protecting taxpayers from the unfair burden of bearing the costs of punitive damages under the FCA.

Can they win? In light of this historically strong and unchallenged position, supported by the arguments in *Stevens*, why would the Seventh Circuit in *Chandler* or Anthony Dunleavy hold that the FCA could apply to counties? The answer may be found in the way that the Seventh Circuit structured its holding in *Chandler*.

If one were to hold the *Chandler* decision next to the *Stevens* decision, it appears as if the Seventh Circuit were raising counterpoints to each of the Supreme Court's reasons for protecting states, point by point. Recall that the first rationale for not finding states to be a "person" was the language discrepancy between the different clauses in the FCA. Referencing those same provisions, the Seventh Circuit drew exactly the opposite conclusion but rather, as related to counties.

> The CID provision was added to provide the Justice Department with a new weapon to discover fraud and investigate false claims suits. That section defines "person" as "any natural person, partnership, corporation, association, or other legal entity, including any State or political subdivision of a State." The CID's definition of person at least demonstrates that Congress intended that states and their subdivisions be potential targets of false claim investigations.

Although the Seventh Circuit acknowledged the Supreme Court's argument that without express language, there is no clear intent on the part of Congress to include a governmental entity, the Seventh Circuit alluded to the glaring question. Why would Congress explicitly allow the Attorney General to conduct FCA investigations on governmental entities and then prohibit further action under the FCA if the investigation revealed false or fraudulent claims?

Recall also that the second rationale by the Supreme Court in *Stevens* was that historically, governmental entities were not subject to punitive damages. The Seventh Circuit addressed this by referencing the underlying policy behind this historical phenomenon. Recall from the *Garibaldi* decision, the argument that levying punitive damages would result in the taxpayer bearing the burden of paying the punitive damages vis-à-vis increased taxes to compensate for the damages. Furthermore, the lack of limitations on the amount of punitive damages allows juries unfettered discretion to impose exorbitant damages, which, in turn, would be an even greater burden on the taxpayer.

The Seventh Circuit, having raised these policy considerations, countered them by indicating that the unjust benefit derived from a FCA violation by a governmental entity would have already been conferred on the taxpayer. Furthermore, the language of the FCA's punitive damages clause limits the award under the punitive damages clause. Finally, punitive damages under the FCA are not assessed by juries but rather by judges who are well versed in these policy considerations, thus imposing safeguards from the kinds of concerns that belie the reasons for prohibiting governmental entities from being liable under the FCA.

Finally, in addressing the third point, the Seventh Circuit makes note of several statutes that allow liability against governmental entities, particularly counties and municipalities. However, the Seventh Circuit makes a distinction with regard to statutory comparisons with regard to counties and municipalities. The court notes that the constitutional issues that arise from holding state agencies liable do not arise in the context of "lesser entities" such as counties. Specifically for example, the Seventh Circuit notes that unlike many Congressional acts that reference Section 5 of the Fourteenth Amendment as a basis for expressly including states, acts that apply to counties and municipalities need not be linked to such constitutional provisions.

Adopting much of the *Chandler* reasoning, Dunleavy argued the impracticality of excluding counties and municipalities from FCA liability. Broadly, Dunleavy points out that federal funding of county and municipal programs taps into a large budget: "Federal funds distributed to state and local governments for such programs as low income housing, education and public safety exceed $200 billion annually. That level of funding creates enormous opportunity — and enormous temptation — for fraud by counties, and the FCA is the weapon Congress has created to combat that fraud." Furthermore he indicated that in light of the federal assistance that is being distributed to cities affected by the aftermath of the events of September 11, 2001, there is greater need for oversight that can only be provided through accountability through the FCA.

> The catastrophic attacks of September 11, 2001, have caused the need for disaster relief and public safety assistance to cities to skyrocket. In New York alone, the federal government has provided billions of dollars to assistance since September 11. Local governments have also sought dramatic increases in federal funding to assist in airport security, increased police presence, and other safety issues. With this increased funding comes the need for increased oversight of federal spending. The FCA is the strongest tool available to detect and deter fraud on the federal fisc, including fraud by counties and other local government entities.

Sovereign immunity. The *Stevens* case left out whether state entities enjoyed sovereign immunity protection from the FCA because the answer to the preliminary question made answering the question of sovereign immunity moot. However, the issue may arise in the *Chandler* case should the Court hold that the FCA does apply to county and municipalities. Yet, this defense may not carry the day. Historically, the Court has held that Congress must make a clear assertion that it intends to abrogate state sovereignty, however, this same requirement is not mandated in the case of municipal and county entities since they are not constitutionally recognized as separate sovereignties.

Conclusion. Clearly the outcome of the *Chandler* case before the Supreme Court will affect the FCA landscape. On the one hand, the result could eliminate an entire class of potential defendants from whistleblower/FCA suits. On the other, the result could implant a strong defense for many governmental entities, especially governmentally run healthcare entities from FCA liability. But there are broader, more practical implications.

In essence, by granting such immunity, county and municipally run healthcare providers, for example, would not be subject to the level of scrutiny as privately run providers with regard to their billing practices. The importance of maintaining a strong compliance program dedicated to preventing the submission of false claims would be diminished. Thus, in essence, this could create another type of unfairness that would impose a seemingly harsher level of scrutiny on private healthcare entities, requiring them to expend far more resources than their governmental counterparts on a compliance program that must be actively engaged in preventing the submission of false claims. ■

CCH Chicago Bureau, Sept. 2002

"Reverse dumping" fine sticks despite no notice

by Geraldine S. Stroka, J.D., R.N.

Hospitals with specialized services should review their Emergency Medical Treatment and Active Labor Act (EMTALA)-related policies and procedures. In the event that a patient-transfer problem occurs, the hospital could be fined without any recourse.

In August 2002, St. Anthony lost a five-year battle with the United States Department of Health and Human Services (HHS) over its failure to accept a patient transfer requiring its specialized capabilities, known in EMTALA circles as "reverse dumping." Judicial deference to agency determinations and regulation interpretation resulted in the denial of St. Anthony's petition to overturn a Departmental Appeals Board (DAB) determination levying a $35,000 fine for an EMTALA violation.

Specialized services needed. This suit resulted from a 1995 incident involving a severely injured accident victim who was brought to Shawnee Regional Hospital, a small hospital. The Emergency Department (ED) physician determined that the patient required services unavailable at Shawnee. He arranged a transfer to an appropriate hospital, University Hospital, and the patient was placed in an ambulance for the trip, only to return when his medical condition deteriorated.

The Shawnee ED physician, recognizing that the life-threatening trauma injury required surgery, started to stabilize the patient and contacted an air-ambulance service to transport him to University Hospital. When informed of the need for surgery, the University Hospital ED physician said that he was unable to accept the patient due to existing emergency surgeries. St. Anthony Hospital, equipped with the services needed, was called. St. Anthony's ED physician deferred the transfer decision to the surgeon who would perform the operation. The surgeon refused to accept the patient; eventually the patient was transferred via air ambulance, to another hospital.

EMTALA violation. Allegations of an EMTALA violation were brought against Shawnee Hospital and were referred, in accordance with the EMTALA regulations, to an appropriate peer review organization (PRO). Shanwnee was given the opportunity to respond and submit additional information resulting in the determination that it did not have the capacity to stabilize this patient. However, St. Anthony was not given any notice of the PRO proceedings or any opportunity to respond.

The PRO determined that an emergency medical condition existed and transfer was appropriate. In May 1998, the Office of Inspector General notified St. Anthony that it wanted to impose a $50,000 civil monetary penalty (CMP) for failure to accept this patient. Prior to the ALJ hearing, St. Anthony attempted to dismiss the agency's actions stating that it was premature given St. Anthony's peer review rights under EMTALA (42 U.S.C. §1320c-3(a)(16)). In a subsequent hearing, the Administrative Law Judge (ALJ) denied St. Anthony's motion stating that it was unsupported by any EMTALA provision. Following that hearing, St. Anthony was charged with refusing an appropriate transfer, violating the reverse dumping provisions of EMTALA, and was required to pay a $25,000 CMP. The ALJ never considered the applicability of the EMTALA provisions granting a hospital subject to PRO review, like St. Anthony and Shawnee Regional Hospital, certain procedural rights.

DAB Decision. St. Anthony appealed the ALJ's determination to the DAB. The DAB did not address the PRO issue but reviewed the ALJ's decision to see if the findings were "supported by substantial evidence on the whole record." The DAB: (1) overruled the ALJ's conclusion that an individual's medical stability, as defined by EMTALA, was irrelevant in determining if reverse dumping had occurred, (2) upheld the ALJ's determination regarding the patient's stability as supported by substantial evidence, (3) reviewed the PRO's report concluding that the transfer was warranted despite the likelihood of deterioration, and (4) increased the CMP to $35,000.

PRO and transfer-based appeal. St. Anthony's multi-issue appeal centered on two questions: (1) should the agency have sought an expert opinion from the PRO concerning issues relating to the hospital's liability, and (2) applying state law, did St. Anthony refuse an appropriate patient transfer? The standard for review (42 U.S.C. §1320(a)-7a(e)) states that "the findings of the Secretary with respect to question of fact, if supported by substantial evidence on the record considered as a whole, shall be conclusive." The practical application of this standard is that courts must give the agency's interpretation controlling weight unless it is plainly erroneous or inconsistent with the regulation.

The critical issue in this case was HHS's contention that despite its failure to provide St. Anthony notice of the PRO review required under EMTALA, the EMTALA peer-review provisions were satisfied. The Tenth Circuit disagreed with HHS's contention, citing specific EMTALA provisions requiring review before sanctions could be effected, the necessity for a PRO review where a medical opinion is required to determine liability, and a finding that there could not be a determination of patient stability without a medical opinion. Because both parties to the suit agreed that stability of an emergency medical condition was relevant to determine a hospital's liability under EMTALA provisions (42 U.S.C. §1395dd(g) and (d)(1)), it concluded that St. Anthony was entitled to PRO review.

HHS wins despite EMTALA non-compliance. However, despite HHS's admitted failure to comply with the PRO provisions of EMTALA, the Tenth Circuit refused to modify or set aside the agency's determination. The court reasoned that despite the lack of notice to St. Anthony concerning the PRO review, St. Anthony failed to demonstrate that it was prejudiced by its nonparticipation in the PRO process. The opinion continually cites St. Anthony's failure to present evidence before the ALJ and DAB, and also stated that St. Anthony bore the burden of presenting affirmative defenses and any mitigating circumstances. The court then proceeded to review each of the many hospital's contentions under the standard found in 42 U.S.C. §1320a-7(e). ■

St. Anthony Hospital v. United States Department of Health and Human Services, 10th Cir., No. 00-9529, Aug. 28, 2002, ¶801,034