CCH Healthcare Compliance LETTER

Volume 6, Issue 19 www.cchgroup.com September 29, 2003

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 Raio G. Krishnayya, Coordinating Editor, at krishnar@cch.com. For more information about the CCH Healthcare Compliance Portfolio visit our online store at http://health.cch.com.

Final EMTALA rule issued

by Raio G. Krishnayya, J.D.

On September 9, the Centers for Medicare and Medicaid Services (CMS) issued a final rule detailing a healthcare provider's obligations with regard to patient requests for emergency medical services pursuant to the Emergency Medical Treatment and Labor Act (EMTALA). According to CMS, the primary purpose of the Rule was to "expand the definition of emergency department." However, for many, the most controversial aspect of this rule deals with the issue of "on call" specialists.

Background. According to CMS, this Rule was promulgated in the wake of a Special Advisory Bulletin issued in November of 1999. That Bulletin sought to clarify issues with regard to dual staffing, prior authorization, the use of financial responsibility forms and advanced beneficiary notifications, as well as issues surrounding payment for emergency medical services. The issuance of the Special Advisory Bulletin was prompted by a number of reports that managed care plans were requiring beneficiaries to seek "prior authorization" from the plan before receiving emergency medical services. EMTALA prohibits Medicare/Medicaid entities from seeking this "prior authorization" vis-à-vis a prohibition against inquiring about a patient's ability to pay for the services. Nevertheless, in cases where hospitals were requiring "prior authorization," the beneficiaries were held personally liable for the costs of the emergency services.

CMS's response was as follows.

> A reasonable argument can be made that patients (other than those arriving in dire condition) should be informed when they request emergency services of their potential financial liability for services. Notwithstanding the terms of any managed care agreements between plans and hospitals, the anti-dumping statute continues to govern the obligations of hospitals to screen and provide stabilizing medical treatment to individuals who come to the hospital seeking emergency services regardless of the individual's ability to pay.

Although the purpose of the Special Advisory Bulletin was to clarify the CMS position with regard to the issue of "prior authorization" as related to EMTALA obligations, the Bulletin seemed to generate further inquiry rather than resolve the issue. For example, issues surrounding when conditions of participation (CoP) must be adhered to versus a provider's EMTALA obligations became a top query. In addition, issues of EMTALA applicability to "on call" specialty physicians and to hospital-owned ambulance services also arose.

In May of 2002, CMS responded by issuing a proposed rule, attempting to further clarify a provider's EMTALA obligations with regard to these issues. Specifically, CMS articulated primarily what was already understood as the core EMTALA

requirement. Providers could not delay emergency screenings or stabilization to determine the beneficiary's ability to pay for the services rendered. CMS *did*, however, indicate that providers *could* contact primary care physicians to seek information pertaining to treatment issues. Furthermore, CMS proposed concurrent authorization—a situation where the provider would inquire about a beneficiary's ability to render payment *without* any delay in rendering screening or stabilization services. While some commenters disagreed with this approach, CMS maintained that discretion to determine when stabilization had occurred would reside with the provider.

Also noteworthy was that the Proposed Rule articulated that an emergency physician would not be precluded from contacting the patient's primary care physician, so long as the contact did not "inappropriately delay EMTALA-mandated screening or stabilization." This language caused some in the medical community to protest because the provision was viewed as interfering with physician-to-physician contact and could expose the provider to EMTALA liability not otherwise contemplated under the statute. However, CMS seemed unfazed by these complaints, asserting that this language was consistent with the intentions of EMTALA's framers and that the risk of erroneous EMTALA prosecution would be minimal. The Final Rule includes no changes to this provision.

Current provisions. According to CMS, the Final Rule was drafted to clarify certain EMTALA provisions; however, to some, this issuance merely adds controversy to an already controversial set of laws and regulations. The provisions of the Rule become effective on November 10, 2003. Outlined below are some of the final provisions and clarifications:

- **Emergency department.** This definition has been expanded to include "any department or facility of the hospital, whether situated on or off the main hospital campus, that (1) is licensed by the state as an emergency department; (2) is held out to the public as providing emergency services without requiring an appointment; (3) during the previous calendar year, has provided at least one-third of all outpatient visits for the treatment of emergency medical conditions on an urgent basis."
- **On call lists.** Probably one of the most controversial provisions of the Final Rule, this provision articulates the standard by which hospitals must maintain "on call" lists. According to CMS, hospitals would have discretion to develop "on call" lists consistent with community standards. In addition, the Rule would allow physicians to be "on call" at more than one hospital as well as allow them to schedule elective surgery during those periods while "on call."
- **Hospital-owned ambulances.** This provision allows hospital-owned ambulances to conform with local community protocols for responding to emergencies. The emphasis is to ensure that cumbersome EMTALA rules do not delay emergency medical services.
- **Off-campus medical services.** The Rule seeks to relax EMTALA restrictions on off-campus health facilities. According to the Final Rule, these types of facilities would be subject to Medicare CoP rules. However, if the facility routinely provides emergency care services, EMTALA would apply.
- **Controversy.** CMS maintains that the Final Rule is merely a clarification of EMTALA requirements. Furthermore, the agency has asserted that the adoption of this Final Rule will help facilitate emergency care services. "We believe this regulation will help to ensure that emergency departments and specialty physicians are there for those who need them," stated CMS Administrator Tom Scully.

Others have disagreed. According to Stephen A. Frew, J.D., a risk management consultant for Physician's Insurance Company of Wisconsin and currently Publisher for the Health Law Resource Center, "There is a real question whether the regulations will actually lessen the burden on hospitals—that is especially true for hospitals in states with EMTALA-like laws and regulations which still control." He further noted that the "on call" provisions could irritate physicians seeking to reduce "on call" obligations.

Generally, it is well understood that the intent of the EMTALA requirements is to ensure that access to emergency services is not delayed due solely to financial ability to pay for such services. Furthermore, courts have almost unanimously held that EMTALA is not a federal substitute for

continued on page 3

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.

EMTALA (cont.)

medical malpractice laws. See e.g., *Hunt v. Lincoln County Memorial Hospital,* 317 F.3d 891 (8th Cir., Jan. 29, 2003).

However, provisions such as the "on call" standard could provide a basis for suit on the premise that the absence of a particular specialist to be "on call" violated "community standards." On the other hand, such cases are difficult to prove because the evidentiary requirement to illustrate the "community standard" is not well-defined, hence the outcome of such cases is highly tumultuous at best.

Moreover, as Frew aptly points out, the issue of preemption arises especially in states that have EMTALA-like statutes that impose similar requirements. Differentiating overlapping provisions and then sorting out the issue of preemption is tedious and could involve costly litigation.

These issues, however, are relevant to many healthcare-related laws and regulations and not only with regard to EMTALA. How this Final Rule will be enforced—the focal point of concern for any provider—remains to be seen.

A copy of the CMS press release can be found at http://www.cms.gov/media/press/release.asp?Counter=837. A copy of Stephen A. Frew's remarks pertaining to the new EMTALA rule may be found at http://www.medlaw.com/reganalysis.htm. ■

Final Rule, 68 FR 53222, Sept. 9, 2003, ¶950,007

Fraud & Abuse

Doctor receives maximum sentence for healthcare fraud

by Sharon Sofinski

Dr. Chijioke Victor Okoro has been sentenced to 151 months in federal prison for healthcare fraud, the U.S. Attorney's Office in Houston announced. The sentence is the maximum prison term under U.S. sentencing guidelines. Okoro also has been ordered to pay $525,000 in restitution to Medicare and private insurers, and a $6.25 million fine.

In October 2002, a jury convicted Okoro of mail fraud, healthcare fraud, and filing false tax returns.

Mail fraud. The fifteen counts of mail fraud resulted from the false bills Houston Medcare, Okoro's sole proprietorship, submitted to auto insurance companies. Okoro received one-third of the settlement paid by the companies.

Evidence presented at trial included taped conversations between Okoro's office manager and two undercover law enforcement officers who were posing as patients. One officer appeared at Houston Medcare for the first time six weeks after the bill for his treatment began. The undercover officers' insurance company was billed for physical therapy treatments they never received. In fact, Okoro never even examined the officers.

Okoro was caught on tape telling the officers' insurance representative that the officers did indeed receive treatment for automobile accident injuries. Houston Medcare's office manager, Ernest Akpan, was previously sentenced to 41 months in federal prison for participating in the mail fraud.

Healthcare fraud. Okoro employed "foreign medical graduates," who were not licensed to practice medicine in Houston or any other state, to perform patient evaluations. However, Okoro told representatives from the insurance companies that he actually performed the evaluations and provided most of the physical therapy himself.

By January of 2000, Okoro had contracted with 14 physical therapy clinics in the Houston area to supervise each clinic's physical therapy services, on-site. Though his signature appeared on patients' medical records, indicating that he either performed their physical evaluation and physical therapy, or supervised their therapy, he was also working full-time in the emergency room and full-time at Houston Medcare. In addition, he was in Nigeria during some of the times he alleged to have been treating patients at the clinics. According to the U.S. Attorney's Office, "Okoro banked over $260,000 from the clinic owners for his part in the scheme to defraud Medicare."

Tax. In addition to these fraudulent activities, Okoro also failed false tax returns for 1996 through 1998.

continued on page 7

The preemption question: The relationship of the Security Rules to other federal and state laws

by Harris Beach, LLP

This article is an excerpt from the CCH HIPAA Security Guide. In it, Harris Beach, LLP provides a method for analyzing whether a given law, rule, or regulation now in effect may be preempted and replaced by the Security Rules. For more information on the CCH HIPAA Security Guide, visit http://health.cch.com.

The Security Rules generally preempt (override) contrary provisions of state law, including state law requiring medical or health plan records to be maintained or transmitted in written rather than electronic formats. The statute does, however, provide certain exceptions to the general rule. Specifically, the Security Rules do not preempt state law if the Secretary of HHS determines that a contrary provision of state law is necessary for certain identified purposes to prevent fraud and abuse, to ensure appropriate state regulation of insurance and health plans, for state reporting on health care delivery costs; or if the state law addresses controlled substances. In such cases, the contrary provision of state law would not be preempted by a federal provision of the Security Rules. State laws that are related but not contrary to the Security Rules will not be affected. The proposed rules did not provide for a process for making exception determinations; rather, a process was proposed in the privacy rulemaking and was adopted with the Privacy Rules.

The Security Rules further limit the preemptive effect of the federal requirements on certain state laws other than where the Secretary makes certain determinations. For example, the Security Rules provide that state laws for the reporting of disease and other conditions and for public heath surveillance, investigation, or intervention are not invalidated or limited by the administrative simplification rules contained in the Security Rules. Also, the federal requirements do not limit states' abilities to require that health plans report or provide access to certain information. Keep in mind that covered entities may be required to adhere to stricter state-imposed security measures that are not contrary to this final rule.

HHS commented that the Privacy Rules establish standards for the rights of patients in regard to the privacy of their medical records and for the allowable uses and disclosures of protected health information (PHI). The identified concerns were discussed in the Privacy Rules.[1] The Security Rules do not specifically address privacy but will safeguard electronic protected health information against unauthorized access or modification.

The state law preemption analysis regarding the HIPAA Security Rules is similar to that regarding the Privacy Rules, as neither standard completely preempts other state and federal laws regulating the security (or privacy) of health information. Instead of creating a definitive and single security standard, the Security Rules create a minimum security standard, a federal baseline below which patient security cannot fall. For covered entities, the Security Rules' failure to completely preempt all state law provisions dealing with the security of PHI means that compliance with HIPAA security standards requires more than compliance with the Security Rules. It means compliance with *all* other federal and state privacy laws to the extent possible, and careful comparative analysis to determine what law should control any given situation when compliance with all laws is impossible.[2]

Given that certain state law provisions relating to the security will not be preempted by the Security Rules, it is imperative that every covered entity carefully consider the preemption issue when developing and implementing its compliance program.

Generally, the Security Rules preempt only those state law provisions that are contrary to, and less stringent than, the Security Rules. Practitioners, both medical and legal, are left with the task of determining when a state law provision is contrary to and less stringent than the Security Rules and therefore preempted. Though there may be instances when it will be clear whether a provision is contrary to and less stringent than the Security Rules, this will not always be the case.

The HIPAA preemption issue is complicated by the fact that it is driven largely by evolving state laws. Some politicians familiar with the Privacy Rules who have concluded that the protections afforded by the Privacy Rules are not sufficient will follow suit with the Security Rules. In fact, there is a movement in some states to pass "companion legislation" designed to afford health information even greater protections and provide patients even more rights with respect to their own medical records than do the Privacy Rules, and such action may affect the Security Rules. If and when these new proposals are enacted, practitioners must become familiar with and, assuming that the new law is not preempted, become compliant with the new state law provisions. Therefore, compliance with the Security Rules marks only the beginning of the compliance challenge. Compliance programs must continue to evolve if, as is expected, states take up the issue of security in earnest.

The analysis in this article assumes that covered entities are aware of, and in full compliance with, any and all state and federal security laws and regulations currently in effect. From this platform, there are two basic rules, gleaned from the HIPAA preemption provisions themselves, which should dispel some of the preemption angst, answer the majority of preemption questions, and limit the number of instances in which a complicated state law preemption analysis is necessary:

- The covered entity should comply with all applicable state laws, other federal laws, and the Security Rules, unless compliance with all such authorities is impossible.
- If compliance with a state law, other federal law, and the Security Rules is impossible, the covered entity should comply with that provision which affords the most security protection.

In addition to these basic rules, the entity should understand that there are specific areas of health care that states have shown the greatest propensity to regulate. These include mental health, alcoholism and drug abuse, HIV and AIDS, and reproductive health relating to minors. This propensity may or may not impact security, but privacy issues have already surfaced. If these areas of governance continue to expand to address security, a preemption question is likely to arise. The preemption issue will also be present if there are any preexisting state rules.

Common sense and knowledge of regulatory trends will not answer every preemption issue. As such, there is no escape from application of certain principles set forth in the Security Rules in order to resolve difficult preemption questions. What follows is a preemption analysis outline, which serves as a reference tool to assist you in the dialogue with your attorney as you proceed through the preemption thicket to the selection of controlling law.[3]

Much of the preemption section of the HIPAA regulations seemingly deals only with privacy issues. A practitioner should not be misled; the analysis in fact deals with the underlying data and not only its privacy, but also its security. It is therefore critical not to take the term "privacy protection" too literally, as secured data means private data. Despite the language used in the regulation, the analysis remains the same.

Preemption analysis

The presumption in any preemption analysis is that any state law provision that is contrary to a Security Rule is preempted by that Security Rule. This general rule, however, has a number of stated exceptions. Therefore, prior to assuming that the Security Rules preempt a provision of state law, the practitioner must determine if any of the exceptions apply. Specifically, the state law provision is not preempted if:

- The state law is necessary to prevent fraud and abuse related to the provision of or payment for health care; ensures state regulation of insurance and health plans to the extent expressly authorized by statute or regulation; relates to state reporting on health care delivery or costs; serves a compelling need related to public health, safety, or welfare; or relates to the regulation of controlled substances;
- The state law relates to the security of individually identifiable health information and is more stringent than the Privacy Rule; or
- The provision of state law, including all of the procedures established under such law, provides for the reporting of disease or injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation or intervention; or
- The provision of state law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals; or
- The Secretary of HHS has issued an exception determination for that provision of state law. A request for an exception determination may be made by a state through a written request from such state's chief elected official, or his or her designee.

When necessary, the preemption analysis will require a close comparison of the state law provision and the Security Rule and/or Privacy Rule at issue. To assist you in framing the relevant issues and arriving at sensible answers, the following method for analysis is provided. Proceed with caution, and before making a final determination, consult your attorney.

Does the state law provision:

a. provide for reporting disease, injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation or intervention; or
b. require a health plan to report or provide access to information for the purpose of management audits, financial audits, program monitoring or evaluation or facility or individual licensing or certification?

If the answer to either a or b is yes, then the state law provision is not preempted. If the answer to both a and b is no, then continue to the next question.

Does the Practice:

a. find it impossible to comply with both the state law provision and the Security or Privacy Rules; or
b. find that complying with the state law provision stands as an obstacle to accomplishing the full purposes and objectives of the HIPAA Administrative Simplification Provisions or the Security or Privacy Rules?

If the answers to both a and b are no, then the state law provision is not preempted. If the answer to either a or b is yes, then proceed to the next question.

Has the Secretary of HHS determined that the state law provision is not preempted by the Security or Privacy Rules?
If yes, then the state law provision is not preempted. If no, continue to the next question.

Does the state law provision have the specific purpose of protecting the privacy of health information or affect the privacy of health information in a direct, clear and substantial way?
If no, then the state law is preempted. If yes, then continue to the next question.

Does the state law provision prohibit or restrict a use or disclosure in instances in which the Security or Privacy Rules would permit such a use or disclosure?
If no, continue on to the next question. If yes, then:

a. Is the disclosure required by the Secretary of HHS for purposes of determining whether the Practice is in compliance with the Security or Privacy Rules; or
b. Is the disclosure made to the patient who is the subject of the health information being disclosed?

If the answers to both a and b are no, then the state law provision is not preempted. If the answer to either a or b is yes, then the state law provision is preempted.

Does the state law provision, as compared to the Security or Privacy Rules:

a. Permit greater rights of access or amendment to the patient who is the subject of the health information;
b. Provide a greater amount of information to the patient with respect to the use or disclosure of his or her health information or with regard to his or her rights and remedies;
c. Narrow the scope or duration of, increase the privacy protections afforded by or reduce the coercive effects surrounding an authorization for the use or disclosure of health information;
d. Require the retention or reporting of more detailed information regarding the disclosure of health information or require such retention or reporting for a longer period of time; or
e. Provide greater privacy protection to the patient?

If the answer to any of a, b, c, d or e is yes, then the state law is not preempted. If the answers to a, b, c, d, and e are no, then the state law provision is preempted.

Final Thoughts

The foregoing outline is, in essence, a road map with basic questions. The preemption question is strained, however, by to the failure of the Security Rules to deal directly with the preemption issue. The answers to most preemption questions should be apparent after determining whether the state law provision or the Security Rules are more stringent. In practice, however, the application of these questions to certain conflicting provisions may be difficult, and answers may not be obvious. An accurate preemption analysis requires not only a word-by-word parsing of the state law provision, but also a keen understanding of the state law as a whole. Ultimately, the most difficult preemption issues will be determined by state legislatures and courts. Until the legislatures and courts finally determine these issues, it is recommended that entities consult counsel to resolve any questions or concerns as to the controlling law.

Resources

HIPAA preemption is an evolving body of law and will continue to be so as long as individual states continue to legislate in the same areas addressed by the Security Rules. Included below is a list of resources to consult when confronted with preemption issues. None of these resources is intended to replace the advice of legal counsel, but they may serve as valuable reference tools when certain preemption issues arise. Many of the websites listed below currently deal only with privacy issues. However, these sites will most likely expand to address security preemption.

New York State Office for Technology - Central HIPAA Coordination Project (www.oft.state.ny.us/hipaa)

- HIPAA Applicability Evaluation and Agency Designation Guidance (www.oft.state.ny.us/hipaa/HIPAAApplicabilityGuidance.pdf)
- HIPAA Participating Agencies (www.oft.state.ny.us/hipaa/members.htm)

New York State Department of Health (www.health.state.ny.us)

- HIPAA Information Center (www.health.state.ny.us/nysdoh/medicaid/hipaa/hipaamain.htm)
- Access to Patient Records (www.health.state.ny.us/nysdoh/opmc/laws/access.htm)
- Rights to Medical Records (www.health.state.ny.us/nysdoh/opmc/medright.htm)
- Bureau of Emergency Medical Services Policy Statement (www.health.state.ny.us/nysdoh/ems/02-03.htm)
- HIV Reporting and Partner Notification (www.health.state.ny.us/nysdoh/hivaids/hivpartner/intro.htm)

New York State Office of Mental Health - HIPAA (www.omh.state.ny.us/omhweb/hipaa/hipaa_home.htm)

- Statewide Privacy Comments (www.omh.state.ny.us/omhweb/hipaa/)
- HIPAA Awareness and Education Course for Business Associates (www.omh.state.ny.us/omhweb/hipaa/training/)

New York State Insurance Department, Privacy Section of the Office of General Counsel (www.ins.state.ny.us/rprvindx.htm)
- Privacy Opinions (www.ins.state.ny.us/rprvopns.htm)
- Privacy Regulations (www.ins.state.ny.us/rprvregs.htm)
- Privacy Circular Letters (www.ins.state.ny.us/rprvcls.htm)

New York State Office of Alcoholism and Substance Abuse Services (www.oasas.state.ny.us/hps/hipaa/hipaa_home.htm)
- HIPAA (www.oasas.state.ny.us/hps/hipaa/hipaa_home.htm)
- New York State Education Department (www.nysed.gov)
- VESID Confidentiality Policy (www.vesid.nysed.gov/policies/102.htm)
- An Implementation Package for HIV/AIDS Policy (www.emsc.nysed.gov/rscs/chaps/HIV/Policy_Implementation_Package.doc)

New York State Consumer Protection Board (www.consumer.state.ny.us)

Medical Society of the State of New York, HIPAA (www.mssny.org/HIPAA/HIPAAindex.htm)

New York State Psychiatric Institute (www.nyspi.cpmc.columbia.edu)
- Policy and Procedure Manual - Confidentiality of Patient Contact (www.nyspi.cpmc.columbia.edu/socialwork/sw1280.htm)
- Policy and Procedure Manual - Patient Rights (www.nyspi.cpmc.columbia.edu/socialwork/sw1242.htm)

Georgetown University Health Privacy Project (www.healthprivacy.org)
- State Health Privacy Laws (www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm)
- New York State Privacy Laws (www.healthprivacy.org/usr_doc/NY2002.pdf)

HIPAA Gives: Government Information Value Exchange for States (www.hipaagives.org)
- White Paper: Tactical Implementation for HIPAA Compliance - State Governments (www.hipaagives.org/uploaddocument/resources/State_Gov_White_Paper_HIPAA_Implementation_v3.doc)

National Governors Association (www.nga.org)
- Issue Brief: HIPAA and the States: Critical Issues and Compliance Strategies (www.nga.org/cda/files/HIPAA052802.pdf)

Electronic Privacy Information Center (www.epic.org)
- Medical Record Privacy (www.epic.org/privacy/medical)
- Privacy Laws by State (www.epic.org/privacy/consumer/states.html)

Electronic Frontier Foundation (www.eff.org)
- Privacy - Medical and Psychiatric Records and Drug Testing (www.eff.org/Privacy/Medical)

Harris Beach, LLP, is a top 250 law firm with offices throughout the Northeast. Since its founding in 1856, it has provided a wide range of legal services for a broad-based clientele. Harris Beach's Health Services Department has been at the forefront of structural changes in the rapidly evolving health care industry. Harris Beach attorneys counsel a wide variety of institutional and individual health care providers, multi-provider organizations, managed care organizations and insurers, and have substantial experience in integrated delivery systems and managed care products. Harris Beach's health services include mergers, acquisitions, affiliations, and reorganizations; general corporate; antitrust; regulatory compliance; operations' medical malpractice defense and risk management advice; labor and employment issues; third party reimbursement; financing services; tax, pensions, and employee benefits; and real estate and environmental issues. They regularly provide compliance advice regarding the privacy and security provisions of Health Insurance Portability and Accountability Act of 1996 (HIPAA) to a wide range of clients, including skilled nursing facilities, physician groups, large corporations and free-standing surgical centers. Their attorneys prepare consents and authorizations, modify business associate contracts and agreements, and perform structural and organizational evaluations for organized health care operations to achieve and maintain HIPAA compliance.

[1] See 65 FR 82587 through 82588.

[2] This article provides a method for analyzing whether a given law, rule, or regulation now in effect may be preempted and replaced by the Security Rules. Determining whether any one provision of law is preempted by the Security Rules requires legal analysis, and a final determination should be made only with the assistance of your attorney.

[3] Keep in mind, however, that a state-by-state, statute-by-statute preemption analysis is not the purpose of this article. Rather, this article provides you with (a) information that will enable you to recognize when a preemption question exists, and (b) a method of analysis, which, with the assistance of your attorney, should prove useful in resolving any given preemptive question.

Fraud & Abuse (cont.)

Three of Okoro's former Houston Medcare employees were convicted separately for their involvement in the scheme. They created the phony paperwork showing that the undercover officers received extensive physical therapy, when in fact they had not. The employees told these "patients" to sign and falsify documents that made it appear that they received more types of therapy—and made more visits—than they actually had.

The FBI, the Office of Special Investigations of the U.S. Department of Health and Human Services (HHS), and the Internal Revenue Service (IRS), Criminal Investigations, collaborated on the case. A copy of the Houston U.S Attorney's Office press release is at http://www.usdoj.gov/usao/txs/releases/September2003/030902-okoro.htm. ■

CCH Chicago Bureau, September 8, 2003

Shareholders as "employees" versus "employers" affect outcome of anti-discrimination cases

by Richard C. Sarhaddi, Esq., Contributing Editor

The federal anti-discrimination acts are designed only to cover employers with a threshold number of employees. For example, to be covered under the Americans with Disabilities Act (ADA) and Title VII of the Civil Rights Act, an employer must have at least fifteen employees; the Age Discrimination in Employment Act (ADEA) requires twenty. Therefore, distinguishing between employers and employees is a critical step in determining whether a business is covered, particularly for smaller operations like clinics and physician practices. This is also true in the context of whether shareholders and directors of a professional corporation could be "employees" for purposes of the ADA, Title VII, and ADEA and other anti-discrimination laws with similar requirements.

The recent case of Ziegler v. Anesthesia Associates of Lancaster, LTD., No. 02-1899, Aug. 29, 2003, (3rd Cir.), was one of the first cases to apply the Equal Employment Opportunity Commission's (EEOC) Compliance Manual factors adopted by the United States Supreme Court in Clackamas Gastroenterology Associates v. Wells, No. 01-1435, Apr. 22, 2003, (S. Ct.) for determining whether a shareholder in a professional corporation is an "employee" or an "employer." In Ziegler, the plaintiffs sued the defendant, a professional corporation, which consisted of 19 shareholder-employees (all anesthesiologists) and 13 non-shareholder-employees (doctors and other staff), claiming sex discrimination and retaliation under Title VII, the Equal Pay Act, and other Pennsylvania state laws. The key issue in the suit was whether the 19 shareholders were "employees" under Title VII, which solely covers employers with 15 or more employees. The district court found that the shareholders were not employees and therefore the plaintiffs' Title VII suit was barred. After deferring its decision pending the outcome of the United States Supreme Court's decision in Clackamas, the Third Circuit affirmed the district court's decision—holding that the shareholders are employers—observing that the district court's analysis closely resembled the Supreme Court's articulated factors. Among the factors employed by the district court to determine the shareholders' status were, whether: (1) the shareholders' share ownership and are accorded equal voting rights in virtually all matters including hiring, termination, offers of partnership and contracting with outside parties; (2) each shareholder makes a capital contribution; and (3) the compensation of shareholders is tied to their performance.

As stated above, the United States Supreme Court in Clackamas, endorsed the factors articulated in the EEOC Compliance Manual in deciding whether four physicians actively engaged in medical practice as shareholders and directors of a professional corporation should be considered employees. See EEOC Compliance Manual §§605: 0008-§§605:00010. The Court noted that the common law element of "control" is "the principle guidepost that should be followed." The EEOC Compliance Manual's factors, which also focus on the issue of "control"in determining the narrow issue of whether a shareholder/director of a professional corporation is an "employee" or "employer," are:

- Whether the organization can hire or fire the individual or set the rules and regulations of the individual's work;
- Whether, and, if so, to what extent the organization supervises the individual's work;
- Whether the individual reports to someone higher in the organization;
- Whether, and, if so, to what extent the individual is able to influence the organization;
- Whether the parties intended that the individual be an employee, as expressed in written agreements or contracts; and
- Whether the individual shares in the profits, losses, and liabilities of the organization.

The Court noted that these factors "are not exhaustive and should take into consideration all incidents of the employment relationship." Clackamas, No. 01-1435, April 22, 2003, (S. Ct.).

Prior to the Court's decision in Clackamas the circuit courts of appeal were divided on how to analyze the issue. The Seventh Circuit applied the "economic realities" test, which assessed the pecuniary relationship between the business and the "employee" to decide employee status. See e.g. E.E.O.C. v. Dowd & Dowd, 736 F.2d 1177 (7th Cir. 1984); the Second (which rejected the "economic realities" test) and Ninth Circuits ruled that a shareholder-employee of a professional corporation is per se an "employee" for purposes of the anti-discrimination laws because he or she is not a "partner." See e.g., Wells v. Clackamas Gastroenterology Assocs., P.C., 271 F.3d 903, 905 (9th Cir.2003); Hyland v. New Haven Radiology Assocs., P.C., 794 F.2d 793, 798 (2nd Cir. 1986); and the Eighth Circuit focused on the shareholders' control and management of the corporation as well as their ownership interest in the corporation. See Devine v. Stone, Leyton & Gershman, P.C., 100 F.3d 78,81 (8th Cir. 1996). The United States Supreme Court's rule in Clackamas resolving the circuit split applies equally to all of the federal anti-discrimination laws containing employee roster requirements.

As evidenced by Ziegler, the Clackamas factors have given courts clearer guidance for determining the status of shareholders in discrimination suits against smaller employers. In addition, the factors give employers that may be near the threshold number of employees the ability to better plan the structure and management of their businesses to help insulate them from being covered by the anti-discrimination laws with employee roster requirements.

CCH Chicago Bureau, Sept. 10, 2003