CCH Healthcare Compliance LETTER

Volume 5, Issue 18 www.cchgroup.com September 16, 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.

Privacy Rule survives another court challenge

by Gordon R. Shea, J.D.

Barely a month after the Privacy Rule component of the Health Insurance Portability and Accountability Act (HIPAA) survived constitutional challenge in a Texas federal court (*see Constitutional challenge to Privacy Rule dismissed*, CCH Healthcare Compliance Newsletter Vol. 5, Issue 13), another court has likewise dismissed a constitutional attack on the rule.

Three-pronged South Carolina attack. This latest court challenge to the Privacy Rule comes from a South Carolina federal court, where the plaintiff South Carolina Medical Association (SCMA) challenged the Privacy Rule on three main grounds:

- that Congress improperly delegated its power to write the Privacy Rule to the executive branch's Department of Health and Human Services (HHS)
- that in writing the Privacy Rule, HHS exceeded the scope of the authority that the text of HIPAA itself vested in the agency; and
- that the Privacy Rule's preemption provision is unconstitutionally vague.

The court challenge was filed long before the Privacy Rule was finalized in August, and the judicial opinion in the case was dated and filed (seemingly coincidentally) on the very day HHS announced it was codifying changes to the rule that it originally proposed in March. Because this latest court opinion addresses the Privacy Rule in general terms – the rule's development and promulgation, and aspects of the rule that have not been the subject of new rulemaking since the Bush administration came into office – it stands as an important document even following the rule's finalization.

Improper delegation, scope exceeded? Addressing the merits of the SCMA's challenge, the Hon. Terry L. Wooten, the judge in the case, concluded that none of the three arguments advanced by the SCMA were sufficient to defeat the rule.

In addressing the argument that Congress improperly delegated power to HHS in making the Privacy Rule, Wooten looked to U.S. Supreme Court precedent indicating that, so long as Congress provided HHS with some "intelligible principle" to guide the agency's drafting of the rule, the rule was acceptable. While Wooten called Congress's delegation of Privacy Rule authority to HHS "not overladen with detailed guidance," he said that Congress's instructions to HHS to design a rule that did not harm federal entitlement programs and did not impede electronic healthcare transactions "provide a sufficient limitation" on HHS's discretion.

Wooten called "important" the next SCMA argument, which was that HHS exceeded the scope of its HIPAA authority by writing a Privacy Rule that governed paper records as well as the electronic records that are seemingly HIPAA's main target. The judge ultimately dismissed this argument as well, however, concluding

that HIPAA's definition of the phrase "health information" may be reasonably read to cover non-electronic records.

Preemption: "troubling." The judge also turned away the SCMA's third line of attack on the Privacy Rule, which centered on the idea that the Privacy Rule's preemption clause – which allows states with "more stringent" privacy laws than HIPAA to disregard the federal Privacy Rule – is unconstitutionally vague. Wooten called this creative line of attack "not sufficiently persuasive" because the rule was adequately clear "as applied to health care providers and to the plaintiffs in this action."

The preemption-based piece of SCMA's challenge was a particularly scrutinized aspect of the SCMA's suit, because the suit provided the first real opportunity for judicial evaluation of the Privacy Rule provision that allows strict state privacy laws to trump the federal Privacy Rule.

Judge Wooten ventured somewhat out on a limb in dismissing the SCMA's preemption challenge on the basis that the Privacy Rule is "constitutional as applied." Wooten wrote that he settled on this approach because, in his view, "it is appropriate to apply a less strict vagueness test" than he might otherwise apply because the "hospitals, physician offices, and health plans" affected by the Privacy Rule are "business interests." As such, the judge said, such entities "are in a position to plan and prepare for compliance carefully through consultation well in advance of" the compliance date of the Privacy Rule. Wooten did not cite any particular legal authority in reaching the conclusion that it might be appropriate to apply a somewhat less strict standard to business interests.

Though the judge dismissed the SCMA's overall challenge, he also pointed to some notable problem areas in other parts of the Privacy Rule's preemption language. For example, Wooten noted that "there is some question as to whether or not a criminal prosecution would lie for making the wrong decision about following federal or state privacy laws." According to the judge, it is "not clear" whether someone "could be prosecuted for making the wrong judgment call as to whether state law is 'more stringent' than federal law" – a situation that Wooten called "somewhat troubling." Referring to a brief that HHS filed as the defendant in the case, Wooten noted that HHS seemed to "acknowledge the possibility of prosecution if a person cannot 'discern' correctly" whether to use state rather than federal law. In addition, the judge said that he could not "lightly dismiss" the SCMA's concern that the Privacy Rule was worded too vaguely to offer providers a reasonable opportunity to know precisely what conduct HIPAA prohibits. Ultimately, however, he held that "the plain and ordinary meaning of the term 'more stringent,'" while "not precisely clear and easily applied in all situations," was sufficiently clear.

(The issue of preemption and the Privacy Rule will be addressed in greater detail in a future *On The Front Lines* article in an upcoming edition of the CCH Healthcare Compliance Newsletter.) ■

CCH Chicago Bureau, September 6, 2002

Hackers, WEDI raise HIPAA-related computer data concerns

by Gordon R. Shea, J.D.

As the healthcare compliance community looks ahead to finalization of the Security Rule and other matters that will affect the safety of data covered by the Health Insurance Portability and Accountability Act (HIPPA), the sensitive nature of healthcare data transmissions is increasingly becoming an issue. Two recent developments – one involving a computer threat report, the other involving the Workgroup for Electronic Data Interchange (WEDI) – have brought the issue to the fore.

667 attacks. The first development is the release of the most recent Riptech Internet Security Threat Report. According to that report, surveyed healthcare entities were victims of a total of 667 computer/Internet hacker attacks during the first six months of 2002. This put healthcare companies toward the middle to lower end of the spectrum in terms of the number of hacker attacks suffered compared to other industries. On the high end was the power and energy industry, which suffered nearly 1,300 hacker attacks during the same period; on the lowest end was the manufacturing industry, which suffered 617 attacks.

The good news for the healthcare industry is that it experienced the lowest number of "severe" hacker invasions of any industry surveyed by Riptech, with only nine percent of healthcare companies reporting severe attacks. Riptech classifies attacks as "severe" when the attacks are "emergency" in nature, or of "critical" importance. This

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 $289 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.

is contrasted with attacks that are more "informational" or "warning"-like, such as attacks that are little more than simple data scans, or firewall breaches that do not compromise particular information.

Similarly, only nine percent of healthcare companies reported being the subject of "highly aggressive" attacks – i.e., attacks that were long in duration, triggered a number of different attack signatures, and seemed to target particular companies. This percentage also put healthcare companies toward the low end of the continuum as compared to other entities; at the high end, fully 20 percent of hacker attacks against power and energy companies were classified as highly aggressive.

Still, Riptech reports that hacker assaults in general, across industries, were up 28 percent over the same period from last year, with a projected annual growth rate of 64 percent. The company's report warns that "virtually all statistics indicate that Internet attack activity remains intense, pervasive, and potentially severe."

A copy of the latest Riptech Internet Security Threat Report is available at http://www.riptech.com/securityresources/form_istr2.html. Riptech is a private data security company, and used its own client base to conduct the survey.

WEDI's entreaty. In another HIPAA computer-related development, WEDI has asked the federal government's Department of Health and Human Services (HHS) to strip out the hyphen that is set to become part of the employer identifier numbers (EINs) that healthcare and other entities must use when corresponding about health insurance matters. According to WEDI, the government's requirement that a hyphen be a part of all EINs will force many healthcare providers and payers to completely reprogram their electronic systems. A copy of the WEDI letter on this matter is available at http://www.wedi.org/public/articles/index.cfm?Cat=235 (click on CMS-0003-P).

EINs are assigned to all employers by the Internal Revenue Service (IRS), which is required by federal regulations to include hyphens within the numbers. Accordingly, when a Final Rule was published on May 31 of this year to address HIPAA's requirement that Standard Unique EINs be made consistent across the healthcare industry, HHS followed IRS policy and federal regulations by mandating the inclusion of hyphens within Standard Unique EINs.

The problem? The May 31 Final Rule seems to contradict HIPAA implementation Guides adopted earlier by HHS. The Guides suggest that HIPAA transactions would be more efficient if the need for any special characters – such as hyphens – was eliminated. According to WEDI, many healthcare entities have already programmed their electronic recordkeeping systems not to accept hyphenated EINs, in reliance on the HHS's original Guides.

The good news for the healthcare industry is that it experienced the lowest number of "severe" hacker invasions of any industry surveyed by Riptech, with only nine percent of healthcare companies reporting severe attacks.

WEDI is a private non-profit group based in Reston, Virginia that describes its mission as fostering "widespread support for the adoption of electronic commerce within healthcare" by such avenues as assisting "healthcare leaders to define, prioritize and reach consensus on the critical technical and business issues which affect the implementation and value of electronic commerce" and ensuring "that electronic commerce standards, policies and regulations for healthcare are thoughtfully developed and implemented." What separates WEDI from other commentators on the HIPAA scene is §1172(c)(3)(B) of HIPAA itself, which endows the group with status as a standard-setting organization for purposes of HIPAA implementation. Because the group is therefore essentially an official advisor to HHS on HIPAA matters, its recommendation about the final rule on EINs and hyphens can be expected to carry some weight as the government nears finalization of HIPAA transaction and code set matters. ■

CCH Chicago Bureau, Aug. 8, 2002

On The Front Lines

When the planet (or its occupants) turn hostile: The role of healthcare human resource managers in disaster readiness

by Judith A. Tichenor, JD, LCSW

Whether part of the solution or part of the problem, healthcare facility managers play a paramount role in the preparation for and management of disasters. Healthcare human resource managers, in particular, are pivotal in the planning and execution phases of disaster readiness once catastrophe strikes.

At the 38th Annual Conference & Exhibition of the American Society for Healthcare Human Resources Administration (ASHHRA) of the American Hospital Association (AHA), four voices of experience spoke on disaster readiness. Their message was consistent across the panel: thorough preparedness must be taken seriously, and it lies in the hands of all levels of executive management. Ira Warm, Vice President, Human Resources, NYU Medical Center, New York, New York, presented the insights he garnered from the bombing of the World Trade Center on September 11, 2001. Lynwood Brooks, Vice President, Human Resources, St. Patrick's Hospital, Missoula, Montana, set out recommendations based on his experiences during the 1995 bombing of the Murrah Federal Building in Oklahoma City, Oklahoma. He added additional wisdom gained in 1999 after the city endured the siege of an F5 tornado that, in tandem with a super cell of tornadoes, ripped through the state for two straight hours. Carl Gustafson, Vice President, Human Resources, of Baptist Health System, Miami, Florida, offered ideas based on his work in several disasters, including the blowout of Mount St. Helens in Washington state in 1980, the San Francisco earthquake in 1989, and Florida's Hurricane Andrew in 1992.

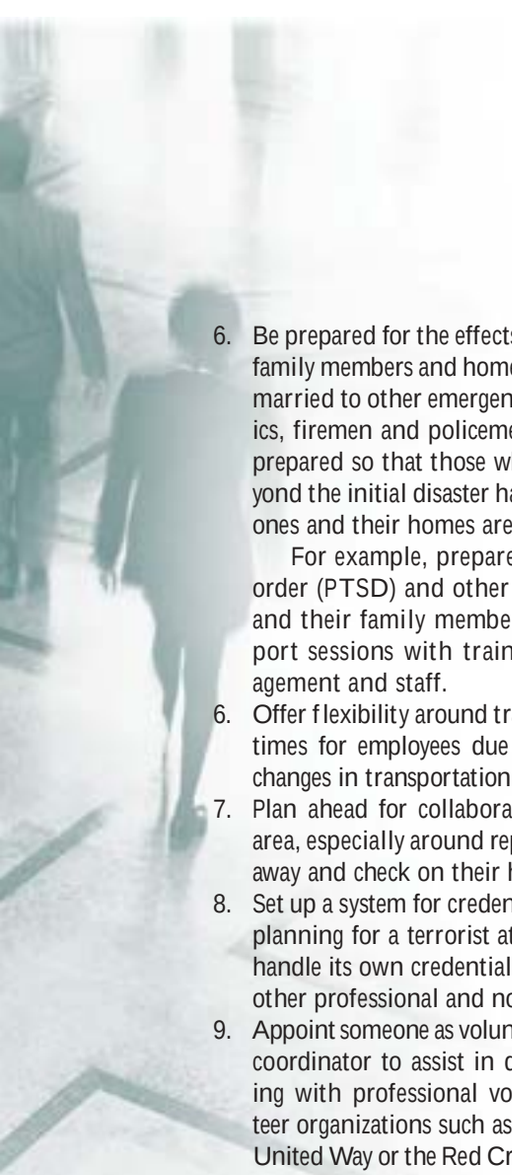
Citing his own professional experience, Brooks said that, during the aftermath of both the Murrah bombing and the Oklahoma City tornado, "the worst disaster was the disaster plan" as far as the healthcare management level was concerned. "Clinicians knew what to do, but regular administrative and management personnel did not," he added.

Not only do managers need to be ready for crisis management when major disaster strikes, but they must be ready for anything, including a change in roles, according to the panel of experts. An alternative leadership may develop, they indicated. Rather than directing the flow of benefits, for example, HR management may find itself directing the flow of water, literally by carrying buckets and waste cans full of it from one floor to another. Others will organize the cadre of volunteers who appear at the hospital into functional, contributing units. Still other managers may find themselves creating employee and family support systems, as well as effective communication networks for employees and their families.

The four panelists agreed that the most critical factors to successful disaster readiness are the people HR hires to fill vacant hospital positions at any level, before a disaster occurs. "Healthcare people are *really* good and *really* care, and we don't celebrate that enough," Brooks observed, to a round of applause. He added, "When the bomb (at the Murrah building) went off, they were there. You can't buy that, but you can build on that, and you should try to do that as much as possible."

The panel offered the following advice and tips to an audience that consisted of primarily hospital and healthcare facility HR managers, generalists and specialists.

1. Be aware of the inevitable shift in focus once the disaster occurs: you are no longer managing a business; you are supporting a clinical care setting. As a result, realize that revenue will be lost.
2. HR's roles should be maximized, both in the planning and execution phases, and at the highest executive level, because, as noted previously, the most valuable resources in disaster management are the people you have already hired.
3. At minimum, three roles will need to be filled:
   - Labor pool initiatives head
   - Coordinator for employees' and victims' families
   - Caretaker of employee needs, including physical, shelter, informational and emotional
4. Martial law may be in effect, which may limit not only freedom of movement, but also supplies of such essentials as gasoline, water, food and clothing. Plan accordingly.
5. Establish plans well ahead of any disaster for an "A" management team and a "B" management team. Twelve-hour shifts were recommended as optimal, with a turnover meeting between each shift to update the incoming managers on the state of affairs.



6. Be prepared for the effects the disaster has on employees' family members and homes. Many medical employees are married to other emergency personnel, such as paramedics, firemen and policemen. Have an information plan prepared so that those who are working extra shifts beyond the initial disaster have a chance to find out if loved ones and their homes are OK.

   For example, prepare for post-traumatic stress disorder (PTSD) and other mental health issues for staff and their family members, and offer educational support sessions with trained counselors for both management and staff.
6. Offer flexibility around travel and work arrival/departure times for employees due to the likelihood of dramatic changes in transportation and access to and from work.
7. Plan ahead for collaboration between hospitals in the area, especially around replacing staff so that they can get away and check on their homes and families.
8. Set up a system for credentialing volunteers, especially in planning for a terrorist attack. While nursing will likely handle its own credentialing, HR will need to credential other professional and nonprofessional volunteers.
9. Appoint someone as volunteer coordinator to assist in dealing with professional volunteer organizations such as the United Way or the Red Cross, especially to provide on-the-spot training to set realistic expectations as to their actual role. For example, many volunteers may arrive expecting to assist with patient comfort, when in reality, they are needed for food preparation or sanitation tasks.
10. Prepare for the likelihood that the employees who are present at the time the disaster occurs will have to be relieved, and set plans as to how that will be accomplished. Determine in advance how employees who fail to show up or return will be managed once the crisis is over.
11. While one panelist acknowledged that a few employees wanted to know about overtime pay, the vast majority of medical employees, both union and nonunion, never asked. Specifically, union demands for overtime pay or additional time off never occurred during the attacks on the World Trade Center, according to Warm. However, he advised having a policy in place in advance of a disaster.
12. On a related note, set up paid-time-off arrangements, allowing for a flexible plan for donation of time-off from employees who were not there during the disaster to those who served overtime but have no time-off available.
13. Develop donations to cover employee's needs, such as home repairs, food, and child and elder adult care, so that dedicated employees can stay and work in the weeks beyond the initial disaster without anxiety or worry.
14. Prepare for nonpatients who will come to the hospital in need of services other than medical treatment. Have a triage plan in place so that their needs can be identified quickly and referred to appropriate agencies and resources.
15. Additional lessons learned from the various disasters the panelists encountered:
    - Have hard copies of employee's names, addresses and phone numbers, since electrical, and therefore computer, systems may be down or utilized only for patient care needs.
    - Learn what is missing in your disaster plan from "everyday disasters."
    - Orient new employees to the disaster plan, with regular retraining, to help ensure readiness.
    - Evaluate the 24/7 human resources capabilities, and plan for all shifts.
    - Make a routine effort to recapture 100 percent of all identification cards and badges from terminated employees. Otherwise, police and security officers will have to put employees through more stringent identification procedures in order to assure patient and employee safety, thus slowing down the deployment of essential personnel.

...the most critical factors to successful disaster readiness are the people HR hires to fill vacant hospital positions at any level, before a disaster occurs.

After the disaster is over, find funds, time and ample opportunities to show gratitude to all hospital staff, including the HR department's own employees, for all their sacrifices, contributions and efforts. For example, Brooks and his fellow managers collected funds and established a monument for all the staff who assisted during the Murrah disaster. A memorial was established as well, but Brooks felt it was essential to acknowledge the unique contributions of the living during that desperate time of need.

The ASHHRA conference was held in Atlanta, Georgia, from July 26 to July 31, 2002. The session on "Executive Update: Disaster Readiness" was held on July 31, and was moderated by Sharon Andre, Director of Education, Martin Memorial Health Systems, Stuart, Florida.

Judith A. Tichenor is an attorney writer/analyst for CCH. Before joining the Healthcare Compliance team, she was an attorney and mediator concentrating in employment discrimination, employment relationships, and mental health law. Prior to becoming an attorney, she was a licensed clinical social worker in private practice focusing on the assessment and treatment of psychiatric disorders. She also served as medical social worker, volunteer coordinator, and bereavement program coordinator for the first JCAHO-accredited, Medicare-certified home health hospice in the United States.

OIG Bulletin: Caution about remuneration

by Raio G. Krishnayya, J.D.

Healthcare providers considering incentive programs for Medicare or Medicaid beneficiaries are urged to take heed of a recent Office of Inspector General (OIG) Special Advisory Bulletin. In the bulletin the OIG reminds providers that pursuant to §1128A(a)(5) of the Social Security Act:

> A person who offers or transfers to a Medicare or Medicaid beneficiary any remuneration that the person knows or should know is likely to influence the beneficiary's selection of a particular provider, practitioner, or supplier of Medicare or Medicaid payable items or services may be liable for civil money penalties (CMPs) of up to $10,000 for each wrongful act.

The bulletin follows in the wake of the recent changes to the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (*see Privacy Rule finalized; most proposed changes codified,* CCH Healthcare Compliance Letter, Vol. 5, Issue 16, Aug. 19, 2002). Specifically, the Department of Health and Human Services modified provisions under the marketing standard to require providers to obtain a patient's written authorization to use protected health information for "face-to-face encounter[s] or a communication involving a promotional gift of nominal value." However, possibly in anticipation of a major shift by the healthcare industry to become HIPAA compliant, the OIG issued this special bulletin to remind providers of the legal limitations regarding "promotional gift[s] of nominal value."

Generally, offering valuable gifts to beneficiaries with the intent to influence Medicare and Medicaid beneficiaries' choices of healthcare provider is a violation of the anti-kickback statute (under 42 CFR 1001.952) as well as other laws and regulations. However, realizing the joint impact of the HIPAA marketing practices and anti-kickback laws, the OIG has stated general guidelines regarding "promotional gift[s]" to beneficiaries.

First, the OIG has articulated that gifts of nominal value will not be scrutinized for prohibited conduct. In defining the term "nominal value," the OIG has excluded gifts that have a retail value of $10 or less, individually, and $50 or less in the aggregate, per year, per patient. Second, the OIG has indicated that items or services that fall under the safe harbor provisions of the anti-kickback statute will also be exempt from scrutiny as well as the following:

- waivers of cost-sharing amounts based on financial need,
- properly disclosed copayment differentials for health plans,
- incentives to promote delivery of specific preventive care services,
- waivers of hospital outpatient copayments in excess of the minimum copayment amounts.

In addition, the OIG encourages requests for advisory opinions and may solicit comments regarding future exemptions. The message to providers is clear, "any gift or free services to beneficiaries should not exceed $10 per item and $50 annual limits," unless the provider's gift fits an exception or is sanctioned by an express advisory opinion. More broadly, it would seem that providers are being reminded to consider other compliance laws in tailoring compliance programs to become HIPAA compliant. ■

OIG Special Advisory Bulletin, Aug. 30, 2002, ¶154,105

Clinical lab recovers attorney's fees

by Raio G. Krishnayya, J.D.

A recent U.S. Court of Appeals for the Ninth Circuit case has laid a foundation for defendant-providers to recoup attorney's fees, especially when the allegations of fraud are rebutted.

The California Department of Health Services (DHS) initiated an investigation into allegations of Medicaid fraud by Labotest, Inc., a clinical lab entitled to Medicaid reimbursements through California's Medi-Cal program. The investigation resulted in DHS imposing administrative sanctions against Labotest. First, it suspended Labotest's participation in the Medi-Cal program and withheld Medi-Cal payments. Second, DHS prohibited Labotest from participating in the California Planning, Access, Care and Treatment (PACT) waiver program, which provides family planning services to low-income beneficiaries. After unsuccessfully challenging the DHS sanctions through the administrative process, Labotest filed a counterclaim against DHS.

The counterclaim was filed pursuant to 42 U.S.C. §1983, a federal statute that prohibits state interference with a party's constitutional rights. Specifically, Labotest asserted that DHS denied it due process when imposing the administrative sanctions. After filing this claim, DHS lifted some of the sanctions, especially those that related to the Medi-Cal program. The lifting of these sanctions was expressed in a stipulation agreement, which left out the issues of attorney's fees and the sanctions dealing with the PACT program. The court accepted and entered the stipulation agreement into the record.

At issue was whether the stipulation agreement provided a basis for Labotest to recover the attorney's fees. Following U.S. Supreme Court precedent, the Ninth Circuit held that the stipulation agreement allowed for recovery of attorney's fees by Labotest. The U.S. Supreme Court articulated that a party is entitled to attorney's fees if the statute includes an express provision for attorney's fees and if there is a legal change in the relationship between the parties that results in awarding attorney's fees.

Therefore, Labotest's §1983 claim allows for the collection of attorney's fees, thus satisfying the first part of the Supreme Court's test. In addition, the Ninth Circuit noted that the stipulation agreement turned Labotest into a prevailing party as defined under §1983. The fact that the lower court accepted and entered the agreement into the record marked a legal change in the parties' relationship, making Labotest the prevailing party. ■

Labotest, Inc. v. Bonta, 9th Cir., No. 01-56318, July 19, 2002, ¶102,039

Allina defendants request Supreme Court review

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

The *Allina Health Systems, et al. v. U. S. ex rel. Minnesota Association of Nurse Anesthetists* case has traveled the "long and winding road" of the federal judicial system and has now reached the last stop, the U.S. Supreme Court. In this important fraud case, the hospital and physician defendants have filed their request to have the Supreme Court review the decision of the U.S. Court of Appeals for the Eighth Circuit because, according to them, it contradicted established law in several areas.

Torturous journey. The initial case began with an antitrust suit, which concerned the staff reorganization of several hospitals' anesthesia departments. The reorganizations resulted in nurse anesthetists (CRNAs) leaving the hospitals' employment to become anesthesia corporation employees. In 1994, the Minnesota Association of Nurse Anesthetists (MANA) filed suit alleging that the reorganizations were a conspiracy in restraint of trade and were designed to cover up false billing claims submitted to Medicare for anesthesia services. The district court granted the motion to dismiss by the hospitals and physicians and the Eighth Circuit affirmed that decision.

Seven weeks after the antitrust case was filed, MANA, as sole relator, filed a *qui tam* suit under the False Claims Act (FCA) against the hospitals and physicians alleging three different categories of false claims that were billed to Medicare:

- single concurrent cases alleging that both an anesthesiologist and nurse anesthetist were not present in all of the procedures with the CRNA;
- billing for medical direction of concurrent procedures when the anesthesiologist was not present for the patient's "emergence" from anesthesia; and
- misidentifying the number of concurrent procedures occurring.

In addition, MANA alleged improper use of a patient modifier resulting in false underbilling and a conspiracy to submit false claims. MANA mailed a copy of the Complaint to a Medicare office, a week after it was publicly filed and disclosed to the press.

Questions for review. MANA alleged that the defendants, through their billing to Medicare for anesthesia services, knowingly submitted false claims to the government in violation of the FCA, 31 USC §§3729–3733. As part of their challenge, the defendants asserted that MANA did not qualify as an "original source" under FCA law.

Under the FCA, a *qui tam* complaint cannot be based upon a prior public disclosure unless the relator qualifies as an "original source," defined as "an individual who has direct and independent knowledge who has voluntarily provided the information to the Government before filing an action..." 31 U.S.C. §3730(e)(4)(B)(1998).

In their request for Supreme Court review, the defendants questioned whether the Eighth Circuit erred by determining that MANA, as a corporation, was an "original source." The Eighth Circuit concluded that MANA obtained the information through a third party (a member) and as such, met the pre-suit disclosure requirements despite the fact that public disclosure of the information occurred before it reached the government.

As a counterpoint, the defendants questioned whether the Eighth Circuit erred in finding an Article III "case or controversy" over the alleged false claims when there was no injury. The "case or controversy" requirement extends to all cases filed in federal courts in order for the courts to assert jurisdiction over the actual case.

The hospitals and physicians questioned if there was error when the court determined that MANA could prove that they knowingly submitted false claims where no existing regulation prohibited the action, and where the hospitals and physicians relied on government advice in their billing procedures.

Reasons to grant review. The defendants' response to the first question was that the federal courts lacked jurisdiction over this action because MANA was not an "original source" as required under the FCA. They based their argument on the following points: (1) MANA was not an "individual"; (2) MANA did not have "direct knowledge" of the information on which it based its allegations; and (3) the Eighth Circuit deviated from other circuits on FCA's pre-suit disclosure requirements.

The second question to be answered concerned "standing" or MANA's ability to bring the suit. The hospitals and physicians argued that MANA could not bring this suit because the alleged conduct of the hospitals and defendants did not result in any injury.

The third question stating that the decision allowing a relator to proceed when the alleged conduct was not prohibited by any government regulation and their billings were done with government advice was of national importance. The hospital and physicians argued that by allowing this, the Eighth Circuit permitted trial on alleged violations of unwritten rules. The hospital and physicians also argued that the circuits are split on whether relying on the government's advice is an absolute defense to liability under the FCA.

The U.S. Supreme Court will decide on whether it will hear this case this fall. The CCH Healthcare Compliance Letter and Healthcare Compliance Reporter have provided extensive coverage of the *Allina* case. See CCH Healthcare Compliance Letter Vol. 5, Issue 2, Feb. 4, 2002, for the Eighth Circuit coverage, and Vol. 2, Issue 8, April 12, 1999, for the district court coverage. In the CCH Healthcare Compliance Reporter, *Allina* is covered in ¶305,094 (3/3/1997), ¶105,035 and ¶300,009 (12/8/1998), and ¶301,442 (1/17/2002). ■

Petition for a Writ of Certiorari, *Allina Health System Corp. et al, v. U.S. ex rel. Minnesota Association of Nurse Anesthetists, U.S. Supreme Court No. 02-27, June 27, 2002,* ¶300,161

AHA issues comment letter on compliance program guidelines

by Patrick J. Osborne

Rick Pollack, American Hospital Association (AHA) Executive Vice President, has issued a comment letter to Janet Rehnquist, Inspector General, Department of Health and Human Services, soliciting information and recommendations for revising the compliance program guidance for the hospital industry, OIG-12-CPG. Pollack opened his letter to Ms. Rehnquist by stating that the AHA, on behalf of its nearly 5,000 member hospitals, health systems, networks and other providers of care, welcomed the opportunity to provide comments to the OIG on the need for revisions to the current Compliance Program Guidance for Hospitals (CPG). The AHA also stressed its appreciation of Rehnquist's review of the CPG and her desire to keep it current with the latest developments in the hospital field. Pollack noted that the AHA and its members were active in the development of the 1998 CPG, and firmly believes that formal compliance programs play a key role in minimizing billing errors as hospitals strive to comply with Medicare's complex legal and regulatory requirements.

Compliance has become part of the hospital culture. Hospitals across the country have established compliance programs and are actively pursuing compliance initiatives. In revising the CPG, Pollack says that "the OIG should recognize the extent to which hospitals have embraced compliance. Individual hospitals have invested significant resources in compliance plans and activities, and the AHA continues to make compliance a focus of the services it provides to members."

In his comment letter, Pollack also noted that some of the current OIG guidance is oriented to the start-up of a compliance program. In the area of training, particularly, the look of the program for new employees or those directly affected by changes in law or regulation will be different than it is for those who have been participating in training for a number of years and are less directly affected by change. The guidance should acknowledge the variety of means through which training can be accomplished (including Web-based or other approaches that do not require face-to-face participation) and give hospitals the latitude to choose what works best within their organizations. This includes recognizing that requiring a minimum number of hours for each employee to be trained is often cumbersome, costly and unnecessary. The guidance should leave the extent of training that is needed to the hospitals' discretion.

The guidance should leave the extent of training that is needed to the hospitals' discretion.

Pollack stressed that compliance programs are established voluntarily as part of hospitals' good faith efforts to meet their legal obligations. However, he also stated that "in the investigations and reporting section, the CPG uses the term 'noncompliance' largely in the context of misconduct." The CPG recognizes that overpayments occur based on mistake or error, not necessarily fraud or misconduct, but the overall tone of the CPG is oriented to fraud and misconduct. In a revised CPG, Pollack and AHA members have urged that the tone be more evenhanded. For example, the return of overpayments should be given equal prominence with the voluntary disclosure process. And guidance on reporting "potential" misconduct should be consistent. Under the current guidance, a hospital is encouraged to report what "may" be a problem, but the protocol seems to assume that all reported matters involve misconduct. An emphasis on the return of unearned payments would reward an effective compliance program and give meaning to the continued recognition by the OIG that instances of fraud are the clear exception.

Finally, Pollack urged the OIG, as it considers changes, to keep in mind the fact that the hospitals using this compliance guidance are diverse in size, location, and complexity. The CPG should make clear that the details it provides are intended as guidance, not as a prescription for a single compliance program that every hospital must follow. In closing, Pollack stressed that the AHA also supports the comments submitted by the Association of American Medical Colleges and the Federation of American Hospitals. A copy of the Comment Letter can be found at: http://www.hospitalconnect.com/aha/advocacy-grassroots/advocacy/comment/cl020819revising.html. ■

CCH Chicago Bureau, August 21, 2002

HIPAA Notice

In a recent statement Ruben J. King-Shaw Jr., chief operating officer of The Centers for Medicare & Medicaid Services (CMS), alerted healthcare providers that the October 16, 2002 deadline to file for an extension for compliance with the HIPAA Transaction & Code Set Standards is rapidly approaching.

The Administrative Simplification Compliance Act (ASCA) allows covered entities a one-year extension as long as they submit their compliance plan by October 15, 2002, either by paper or, preferably, electronically at www.cms.hhs.gov/hipaa/hipaa2/ascaform.asp. Filing electronically is quick and easy, and filers will know immediately that the extension has been received.

By filing for the one-year extension, healthcare providers will have until **October 16, 2003** to become HIPAA compliant. For more information, see CMS's HIPAA website at www.cms.hhs.gov/hipaa/hipaa2.

A copy of the CMS News Release can be found at: http://www.cms.gov/media/press/release.asp?Counter=484