CCH Healthcare Compliance LETTER

Volume 5, Issue 19 www.cchgroup.com September 30, 2002

On The Front Lines 4

"To ends the most public and universal:" Preemption and the Privacy Rule
by Gordon R. Shea, J.D.

Fraud & Abuse 1

- DM web-based management program gets OIG approval
- Registered nurse arrested for Medicaid fraud
- Contributions for cardiology program could be prohibited remuneration

HIPAA 3

- HIPAA Survey: Compliance activity, regulatory headaches up

False Claims 6

- Southcoast fined over $3M to settle overbilling claims
- CHRISTUS Health Gulf Coast to pay $220,000 in whistleblower case

Medical Staff 7

- Patient safety wins—HCQIA immunity upheld

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.

DM web-based management program gets OIG's approval

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

Attention all disease management (DM) companies: A "guidance" on the application of fraud and abuse laws to your corner of the healthcare world is now out! Despite its concerns with many Internet advertising tactics, the Office of Inspector General (OIG) gave its official nod to a web-based patient compliance program. OIG permitted an Internet-based disease management company to provide a drug and behavioral compliance program to the enrollees of managed care companies (MCOs) and health plans despite "banner" advertising, pharmacy hyperlinks, and sponsorships of chat rooms by pharmaceutical companies.

Proposed arrangement. A web-based behavior modification and drug regimen compliance company presented its chronic disease management program proposal to two different arms of the federal government, OIG and the Patent Office. Under the proposed plan, the company would contract with MCOs and health plans to provide an Internet-based compliance program for their enrollees. These enrollees and their physicians would receive points for their utilization of the program. Companies including healthcare firms and pharmacies could buy advertising and marketing opportunities on the program's website.

Behavioral modification program. Utilizing Internet technology, the company would contact members to take medications, refill prescriptions, and comply with physician orders. MCOs would pay for the program through either a fixed fee per member per month or a fee from the savings, measured by predetermined benchmarks, received by the MCOs.

Once a contract existed between the Internet company and the MCO, the MCO would identify potential eligible enrollees from its patient lists for the Internet company to contact. Compliance program participation was voluntary with both patients and their physicians (if the patient requested physician participation) earning points redeemable for goods and services unreimbursable by any federal healthcare program. Participating physicians' role was to review patient information and compliance results. Members in the program would be able to fill prescriptions at any pharmacy but would not receive points for purchases at any pharmacy advertising on the website.

Advertising segment. Banner advertising and other promotional opportunities would be offered to both healthcare (excluding non-MCO network pharmacies) and nonhealthcare advertisers. MCO network pharmacies could establish hyperlinks to their own websites and pharmaceutical companies could sponsor disease-specific chat rooms, with both types of entities having advertising fees fixed at a flat or "per click" rate. All paid advertising would be clearly identified and

distinguished from healthcare content, posted with a disclaimer disavowing any endorsement, and nonexclusive. The Internet company would control all content in the chat rooms.

MCO payment okay. Payments by MCOs did not implicate the anti-kickback statute because the services are not reimbursable under federal healthcare programs. The company's services do not include the provision, referral or recommendation of federal healthcare business other than complying with physician orders and prescriptions. Although the points incentive program constitutes remuneration because compliance should result in lower MCO costs, the compliance program posed a minimum risk of fraud and abuse because the points are not reimbursable under any federal program, and no financial relationships exist between the participating patients or physicians involving federal healthcare program business.

Five-factor analysis. The anti-kickback issue concerned whether Internet advertising by a healthcare provider leaves the impression that the provider is recommending the advertiser's products to its viewers, some of whom would be federal healthcare beneficiaries. OIG reviewed five factors in its analysis: (1) identification of the party engaged in the marketing activity and its relationship with the audience; (2) nature of the marketing activity; (3) item or service marketed; (4) target population; and (5) fraud and abuse safeguards. OIG determined that the proposed program advertising was similar to print advertisement and not targeted at federal healthcare beneficiaries; therefore, it did not arouse anti-kickback concerns. Also, all advertising would be clearly identified as paid advertising.

OIG also conducted a heightened analysis because healthcare providers would be conducting the marketing, known as "white coat" marketing. This type of marketing merits increased scrutiny because healthcare providers, held in a position of trust, may exert undue influence when recommending products, particularly to their own patients. Here the Internet company is a healthcare provider to MCO enrollees as part of their healthcare plan. However, OIG determined that the company's role was limited to the sale of space on a website. Due to omnipresent advertising and all the assurances presented by the Internet company, OIG determined that the viewer would be able to distinguish paid advertising from substantive recommendations. OIG reasoned that as long as the Internet company's advertising fees represent fair market value and do not vary in volume or value of business generated from the advertising, it would not impose administrative sanctions for these fees.

OIG further stated that MCO-participating pharmacies and their hyperlinks would be listed on the member's secured personal web page despite no remuneration to the Internet company for the listing. This listing is considered part of the compliance program purchased by the MCO for the convenience of its members and to promote compliance through the ability to refill prescriptions online. Also, because the Internet company controlled chat room content and the pharmaceutical companies' sponsorship role was clearly identified by an advertising banner, sponsorship of the chat room would be allowed.

Despite permitting this particular proposed program, OIG voiced concerns about Internet advertising and marketing relationships. Some of the concerns were: (1) a webmaster could manipulate this vulnerable population toward sponsors' products; (2) the company could track members' purchasing habits; and (3) misuse of personal information for e-mail and other technologies. ■

OIG Advisory Opinion 02-12, Aug. 30, 2002, ¶150,193

Registered nurse arrested for Medicaid fraud

by Patrick J. Osborne

A registered nurse in Orlando, Florida, was arrested for fraudulently billing her employer for nonexistent visits to Medicaid patients' homes, Attorney General Bob Butterworth announced. Penny Stockford, 49, was charged with 13 counts of Medicaid provider fraud and grand theft, all third-degree felonies. She faces up to five years and a $100,000 fine for each offense. According to Butterworth, Stockford submitted false and fraudulent time sheets to her employer, Pediatric Services of America Inc., showing she had made more than

continued on page 7

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
Craig Arritola

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.

HIPAA Survey: Compliance activity, regulatory headaches up

By Gordon R. Shea, J.D.

The Healthcare Information and Management Systems Society (HIMSS) and Phoenix Health Systems have released their quarterly HIPAA survey for Summer, 2002, finding an upsurge in Security Rule compliance activities, even as regulatory uncertainties continue to dog HIPAA observance generally.

New focus. The survey's executive overview leads off with what HIMSS and Phoenix call a "significant overall trend:" HIMSS and Phoenix report that they "no longer have to ask" if or when respondents will begin HIPAA compliance efforts as part of their four-times-a-year survey. Instead, the focus in the HIPAA world has shifted to interpreting finalized regulations, meeting deadlines, and gearing up for whatever specifics the pending Security Rule may contain.

The survey found that "the biggest roadblocks to HIPAA compliance" are now "potential changes in regulations/deadlines" and the "interpretation of the regulations." This is the first time since HIMSS and Phoenix began tracking numbers in 2000 that concerns other than those related to general awareness and start-up problems topped the list of compliance roadblocks. Anecdotal evidence presented in the survey report also strongly suggests that the seemingly ever-changing nature of HIPAA administrative rules has become one of the biggest frustrations for HIPAA-covered entities.

In another departure from past results, the survey reports that HIPAA compliance programs are now going into areas of "planning implementation and training," and have moved "well beyond" the stage of initial assessment. While HIPAA's Security Rule component has yet to be finalized by the federal government, that rule seems to be an area of increasing attention, with the survey finding what it called an "upsurge" in security compliance efforts.

Deadlines. The HIMSS/Phoenix survey also indicates that, in the increasingly mature HIPAA compliance marketplace, deadlines loom larger than ever. Many survey respondents reported that they will avail themselves of the new deadline extensions that have been offered for bringing Business Associate agreements into line with HIPAA requirements. Eighty-five percent of clearinghouse respondents said that they intend to meet their April, 2003 deadline for the transmission of HIPAA-required transactions. Similarly, most vendor and payer respondents reported that they will be able to transmit required transaction data by their new October, 2003 deadline. Eighty-four percent of total respondents reported that they are already utilizing the government's proffered extension to the Transactions deadline (which was originally set for this October but has now been put off until October, 2003).

This optimism, however, was balanced by other findings, such as those about Business Associate agreements. For example, the HIMSS/Phoenix study found that many covered entities do not believe their Business Associate agreements will be affected much by the Privacy Rule, and many others are confident that the new Business Associates deadline provides them with ample time to reshape those agreements. A significant 27 percent of respondents, however, indicated that the extended Business Associate agreement deadline will have the practical effect of slowing their effort to complete such agreements. And in what the survey reporters termed "The Big Question" of the survey, 78 percent of total respondents said that they have not "generally completed" both HIPAA Transactions/Code Sets and Privacy remediation efforts.

Methodology. The HIMSS/Phoenix survey was conducted anonymously over HIPAAdisory.com, a website run by Phoenix Health Systems. The survey took place shortly after the federal government announced its finalization of most of the changes it had earlier proposed to HIPAA's Privacy Rule. Over 70 percent of survey respondents reported "moderate or strong support" for the elimination of the Rule's prior consent requirements that was the main focus of those changes.

A report of the HIMSS/Phoenix Health Systems survey is available at http://www.hipaadvisory.com/action/surveynew/summer2002.htm. ■

CCH Chicago Bureau, Sept. 19, 2002

"To ends the most public and universal:" Preemption and the Privacy Rule

by Gordon R. Shea, J.D.

As healthcare entities gear up to comply with HIPAA's now-finalized Privacy Rule, they may want to take a step back and consider that, thanks to a legal doctrine known as preemption, the rule may not even apply to them—or may apply only in part.

The saint and poet seek privacy to ends the most public and universal: and it is the secret of culture..
–Ralph Waldo Emerson

The political follies that have gone on ever since the Bush Administration first announced that it was considering changes to the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) have been remarkable.

On one side of the political divide, Senator Christopher Dodd (D-Conn.) said he was "outraged" by the changes before the changes were even finalized. On the other side, industry representatives booed a representative of Georgetown University's Health Privacy Project during March's HIPAA Summit in Washington, D.C., for merely broaching the moderate position that the Privacy Rule as it stood prior to Bush's changes was flawed but not irretrievably broken.

This *sturm und drang* has been, at least potentially, wildly offbase. As healthcare entities gear up for compliance now that the Privacy Rule seems to be really, truly final, they need to consider that, thanks to a legal doctrine known as preemption, the rule may never even apply to them—or may apply only in part.

Preemption law generally

Lost in all the Privacy Rule hand-wringing of this year has been the fact that the rule simply presents what legal experts often call a "floor" of regulations: it sets forth the minimum regulatory requirements under which the federal government will attempt to protect patient privacy.

Under America's federal system of government, states are free to pass laws independent of the national government. Naturally, however, there must be limits on this so that state laws do not come into direct conflict with federal laws. The legal doctrine of preemption comes into play to avert such conflicts by allowing federal law to trump state law under certain circumstances.

Conflict/ordinary preemption. In a "conflict" (also known as an "ordinary") preemption scenario, Congress legislates the area of law in question in a way that is limited, but that gives rise to a clash with given state laws on the same topic. In this situation, state law is allowed to stand alongside federal law, and the two types of law are allowed to operate independently to the extent that they do not overlap.

This has been the Privacy Rule battleground.

HIPAA could be said to have two preemption clauses. The first is at section 1178(2), which says that "a provision or requirement under this part...shall supersede any contrary provision of State law," but "shall not supersede a contrary provision of State law, if the provision of State law...subject to section 264(c)(2) of the Health Insurance Portability and Accountability Act..relates to the privacy of individually identifiable health information." Section 264(c)(2) of HIPAA, in turn, is the second HIPAA preemption clause. It says that a "regulation...shall not" be considered to "supercede a contrary provision of State law, if the provision of State law imposes requirements...that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation." Both these clauses are conflict preemption-based.

During this spring's HIPAA Summit in Washington, D.C., attorneys from the Department of Health and Human Services (HHS) repeatedly stressed that professionals who deal with HIPAA could avoid many problems if they just take the time to carefully read the law. Under this "just read the law" standard, HIPAA's Privacy Rule preemption issue may not seem terribly complicated: states that have medical privacy laws that are stricter than HIPAA's Privacy Rule can disregard HIPAA and go with their own law, while states that don't have medical privacy laws that are stricter than HIPAA's Privacy Rule will be bound by the Privacy Rule. What could be simpler?

It turns out not to be that easy.

Recent Privacy Rule litigation

Two recent, and unsuccessful, federal court challenges to the Privacy Rule demonstrate some of the arguments that can be levelled against the rule:

AAPS. The Association of American Physicians and Surgeons, Inc. (AAPS) recently lost a broad-based attack on HIPAA's constitutionality that included a preemption-based argument that the Privacy Rule "trammels" on the laws of such states as California and Florida.

According to the AAPS, Florida and California law both provide for nearly immediate patient access to medical records. By contrast, HIPAA allows providers up to 90 days to provide such information. Thus, AAPS's argument went, HIPAA actually

establishes more lax standards for medical privacy than are acceptable in some states. The judge in the case disagreed that this was a problem, however, noting that HIPAA's preemption language actually seemed to buttress laws like California's and Florida's. In a footnote, the judge specifically cited HIPAA's preemption language to support his dismissal of the case.

SCMA. A direct assault on the Privacy Rule's preemption language was similarly defeated in South Carolina. In August, 2001, the South Carolina Medical Association (SCMA) filed suit against the DHHS in federal court, directly citing HIPAA's preemption language in hopes of stopping implementation of the Privacy Rule.

Interestingly, the SCMA used what was the preemption "problem" for the AAPS plaintiffs as a potential "solution" for those hoping to defeat the Privacy Rule. While the judge in the AAPS case maintained that HIPAA's preemption language was a reason to uphold the law, the SCMA plaintiffs turned that language against the law itself. According to the SCMA, sections 1178(2) and 264(c)(2) were "impermissibly vague" because they were "unclear which state laws will be preempted by the HHS Privacy Regulations." The SCMA said that the "term 'more stringent' is unclearly defined," such that "a person of ordinary intelligence is left uninformed by the statute if the HHS Privacy Regulations or state privacy law would govern his or her actions." The plaintiffs claimed that "most states, including South Carolina, already have legislation protecting patients' medical privacy" in place. Such legislation, according to the SCMA, "may or may not be pre-empted by the HHS Privacy Regulations" in light of section 264(c)(2).

As reported in the last issue of this newsletter, this challenge, too, proved unavailing, and the Privacy Rule was again upheld. But even as the SCMA lawsuit played out, states already began encountering potential overlaps between their laws and HIPAA. A recent Attorney General's opinion in Texas, for example, not only suggests (in what otherwise seems a complete contradiction of HIPAA's principles) that personal health information should be readily available to parties outside of specific healthcare transactions, but that hospitals *must* send such information to other government actors…and must even do *so without patient consent*.

Which law applies?

With the Privacy Rule's constitutionality and general legality now seemingly beyond question, HIPAA covered entities must now move on to the real meat of the HIPAA preemption problem: how does one know if any given state's privacy laws are looser or stricter than HIPAA—i.e., how does one know if HIPAA applies to them or not?

Bad news. The only way to really answer that question is to compare side-by-side each provision of HIPAA with each relevant provision of the state privacy law.

A close reading of the text of HIPAA's preemption clauses backs that approach. Note how both section 1178(2) and section 264(c)(2) are worded in the singular—they speak in terms of "*a provision*" of state law, "*a* contrary *provision* of State law, if *the* provision of State law" relates to privacy, a "*regulation*" that shall not "supercede *a* contrary provision of State law, if *the* provision of State law imposes" requirements stricter than HIPAA. This means that while some individual provisions of any state's given law will be considered more stringent than HIPAA (and will thus supercede HIPAA), other provisions of the same law may not. The only way to figure out which provisions are more stringent is to do the arduous work of comparison.

There is another piece of bad news: note how HIPAA's preemption clauses speak in terms of state *law*. This strongly suggests that people who compare their state's privacy protections to those found in HIPAA should not confine themselves to their state's *statutes* on medical privacy. Because the word "law" encompasses common law court precedents and administrative provisions as well as statutes, researching any state's privacy "law," as required by HIPAA, may prove to be a monumental task.

The good news. Luckily, some help is available. The Health Privacy Project, a group often vilified for its opposition to the Bush Administration's proposed modifications to the Privacy Rule, issued a general overview of state privacy laws in 1999 and has made surveys of all 50 individual states' (and the District of Columbia's) privacy laws available ever since. Both a general report on the topic and a survey of each individual state's law can be accessed through The Health Privacy Project's website, http://www.healthprivacy.org. The group also recently began updating its state information; as of September, 2002, the HPP had completed updates for the following states: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Indiana, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico New York, North Dakota, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Utah, Vermont, Virginia, Washington, and Wyoming. Users of HPP resources, however, should be aware that the group's survey is confined to state *statutory* law.

For those more inclined to look to an industry-oriented source of help, the American Hospital Association recently created a flowchart and model framework for its members that hospitals can use to conduct or evaluate state preemption analyses.

No matter which tool compliance and privacy officers use to do the hard work of preemption gap analysis, it seems increasingly clear that such officials have been drafted to help protect not only the valued privacy sought by the "saints and poets" Emerson spoke of, but of all those who come in contact with the nation's healthcare system.

Gordon R. Shea is a CCH Compliance Law Analyst and Editor. For more information, you may contact Mr. Shea at (847) 267-2812 or sheag@cch.com.

Southcoast fined over $3M to settle overbilling claims

by Patrick J. Osborne

United States Attorney Michael J. Sullivan and Joseph C. Moraski, Regional Inspector General of the U.S. Department of Health and Human Services, Office of the Inspector General, have announced that the United States has settled civil claims against Southcoast Hospital Group, Inc., formerly Charlton Hospital and St. Luke's Hospital (Southcoast), for submitting false and/or fraudulent claims to Medicare. Southcoast has agreed to pay $3,034,993 for false and fraudulent claims to Medicare in bacterial pneumonia billings.

The agreement settles allegations made by the United States against Southcoast that from October 1, 1992 through September 30, 1995, Southcoast submitted claims to Medicare with the principal diagnosis code of 482.89 for complex pneumonia, due to "other specified bacteria." However, claims under that diagnosis code were not supported by the corresponding medical records. As a result of these claims, Southcoast received reimbursements to which it was not entitled, because Medicare reimburses the treatment of a simpler form of pneumonia at a lower rate.

Medicare payments to the hospital for inpatient treatment rendered to Medicare beneficiaries generally are based upon the beneficiary's "principal diagnosis," as set forth by the hospital in its claim submitted to Medicare. The Medicare program relies upon participating hospitals to properly indicate the principal diagnosis, through the use of standard diagnosis codes.

The case was investigated by the Office of the Inspector General of the U.S. Department of Health and Human Services and was handled by Assistant U.S. Attorney Susan Winkler in Sullivan's Health Care Fraud Unit and Assistant U.S. Attorney Sara Miron Bloom in Sullivan's Civil Division. A copy of the DOJ News Release can be found at: http://www.usdoj.gov/usao/ma/presspage/Aug2002/Southcoast%20Hospital%20Grp-civil%20settlement.htm. ■

CCH Chicago Bureau, Aug. 22, 2002

CHRISTUS Health Gulf Coast to pay $220,000 in whistleblower case

by Patrick J. Osborne

CHRISTUS Health Gulf Coast, owner and operator of CHRISTUS St. Joseph Hospital, of Houston, Texas, has agreed to pay $220,000 to settle claims that the hospital defrauded the Medicare Program from April, 1997 to June, 2000, the Justice Department announced today.

The civil settlement resolves allegations that the hospital defrauded Medicare by knowingly requesting reimbursement for $78,000 in non-recoverable costs at the Garden Oaks and Seabrook Senior Centers, two outpatient senior health clinics formerly operated by St. Joseph Hospital. The hospital improperly billed Medicare for evaluation and management (E&M) services and supplies incident to a physician's services. Recovery of the costs of E&M services provided by non-physicians is limited by applicable regulations. St. Joseph Hospital unlawfully obtained reimbursement for E&M services and supplies provided without the direct personal supervision of a physician, among other violations of the Medicare Part B regulations.

"This settlement again demonstrates the United States' commitment to protecting federal funds from fraud and abuse," said Robert D. McCallum, Assistant Attorney General in charge of the Civil Division. "The federal healthcare system operates on the good faith and honesty of its providers, and we will actively pursue those who misuse the system for financial gain."

The allegations arose from a lawsuit filed by two former employees of the hospital under the *qui tam* or whistleblower provisions of the False Claims Act, a federal law that allows private individuals to sue on behalf of the United States. The whistleblowers' share of the settlement totals $33,000. The lawsuit was unsealed in Houston, Texas.

The civil investigation and settlement were jointly handled by the Office of the U.S. Attorney for the Southern District of Texas and the Civil Division of the Department of Justice, with assistance from the Department of Health and Human Services Office of Inspector General.

The case is entitled *United States ex rel. Connie Kaisler and Thereze Rendon v. Christus Health Gulf Coast d/b/a Christus St. Joseph Hospital,* Civil Action No. 01-CV-1592 (S.D. Tex.). ■

CCH Chicago Bureau, September 6, 2002

Follow Up

Earlier this summer, the CCH Healthcare Compliance Letter reported a controversy about the Indianapolis, Indiana Veterans Adminsitration (VA), which donated computers to a local thrift shop without first stripping sensitive information off those computers' hard drives. (See *Sensitive VA medical and credit info found on $10 computers,* CCH Healthcare Compliance Newsletter, Vol. 5, Issue 11.) A local television news team found the discarded computers on sale for $10 apiece, and from them was easily able to access such records as VA patients' HIV diagnoses, illegal drug use, mental health records, arrest records, and social security numbers. Shortly after the story broke, Indiana Congressman Steve Buyer – who also happens to serve on the House Committee on Veterans' Affairs – issued a press release demanding answers.

While the VA has been rather tight-lipped about the incident, the magazine *Federal Computer Week* now reports that the Department of Veterans Affairs has changed its policies so that it can avoid similar incidents in the future. While the VA has long had a policy mandating the erasure of sensitive information from discarded information technology, and while the Indianapolis incident seems to have clearly violated that policy, *Federal Computer Week* reports that the VA will be adding a certification process for all of its information services officers. This change will be implemented by October, 2003.

310 visits to the homes of both Medicaid and private insurance patients to provide medical services. The false time sheets resulted in unnecessary payments of $11,630.40 by Medicaid to Pediatric Services. Stockford subsequently obtained $7,480 from her employer based on the falsified time sheets. Butterworth commended Pediatric Services for reporting the suspected fraud and its cooperation throughout the investigative process. A copy of the Attorney General's News Release can be found at: http://legal.firn.edu. ■

CCH Chicago Bureau, Aug. 29, 2002

Contributions for cardiology program could be prohibited remuneration

by Sharon Sofinski

A state-chartered hospital's proposal to make charitable contributions to a university endowment association could be prohibited by federal law. According to a recent Advisory Opinion by the Office of Inspector General (OIG), such a proposal might also be construed as prohibited remuneration pursuant to the anti-kickback statute. However, the OIG would not impose administrative sanctions on the hospital authority or the university.

Proposed contributions. The hospital authority proposed to make charitable contributions to the endowment association to develop a comprehensive cardiovascular services program. The hospital authority and endowment association planned to enter into a support agreement by which the hospital authority would make contributions to the association to establish two funds: one for education and research in internal medicine, and one for education and research in the university's school of medicine. The hospital authority would then make the proposed grant in accordance with the support agreement.

The university certified that:

- it would not require or encourage physicians to refer patients to the hospital,
- it would not keep track of referrals from faculty physicians to the hospital,
- compensation paid to faculty physicians would not be related to the number or type of referrals made by faculty physicians to the hospital, and
- the total compensation paid to faculty physicians or any physicians employed by the hospital authority would (1) be set in advance, (2) not exceed the fair market value for the services provided, and (3) not be determined in a way that takes into account the number or type of referrals or other business generated by the physicians for the hospital.

The OIG called the arrangement "as straightforward as it is problematic: it is a substantial donation by a hospital to a major referral source." The university is a referral source for the hospital authority since the university employs and is affiliated with faculty physicians who make the referrals.

Anti-kickback issues. Under the anti-kickback statute, it is a criminal offense to offer, pay, solicit or receive any remuneration with the intent to induce referrals of items or services that are reimbursable by a federal health care program. Accordingly, the OIG stated, the proposed contributions would in fact implicate the statute, and the OIG would have sought criminal sanctions had the intent to induce or reward referrals been present.

However, the OIG would not impose administrative sanctions, citing the following reasons:

- The proposed contributions would be between components of an academic medical center that shared a common heritage as public institutions and a common mission in training physicians and providing medical care. The contributions would be consistent with the parties' "public and charitable mission."
- The contributions are consistent with state legislation that established the hospital authority and required it to support the education, research and public service activities of the medical center.
- The university assured the OIG that it would take steps to protect physician judgment and income from pressure to provide referrals to the hospital. ■

OIG Advisory Opinion 02-11, Aug. 19, 2002, ¶150,192

Medical Staff

Patient safety wins—HCQIA immunity upheld

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

The delivery of safe healthcare, one of the top priorities of the federal government, healthcare regulatory agencies, healthcare institutions, and employer groups, was recently bolstered by a decision affirming immunity for healthcare peer review actions. The motion dismissing the suit, previously granted to Blue Cross and one of its physician-reviewers, was affirmed. The subject of the Blue Cross peer review actions, Dr. Singh, had sued the insurer alleging that the actions violated his rights.

"Reviewed" MD sues. The peer review process for this physician involved (1) two treatment record audits, (2) a remedial action committee (RAC) that recommended his termination in all Blue Cross plans, and (3) a fair hearing that reversed the termination recommendation. Even though his Blue Cross contracts, both health maintenance organization and indemnity, were never terminated, Dr. Singh sued Blue Cross and one of its physician reviewers, Dr. White, for harm resulting from the peer review process. In his appeal, he alleged defamation, torturous interference with advantageous business relations, breach of contract and violation of state law against Blue Cross; against Dr. White, he alleged defamation.

HCQIA peer review immunity. The Health Care Quality Improvement

Act (HCQIA) shields healthcare entities and physicians from liability for damages for their actions in monitoring the competence of healthcare professionals. Immunity attaches to professional review actions under 42 U.S.C. §11112(a) when they are taken (1) in the reasonable belief that the action was in the furtherance of quality health care, (2) after a reasonable effort to obtain the facts of the matter, (3) after adequate notice and hearing procedures are given to the physician or other procedures that are fair to the physician, and (4) in the reasonable belief that the action warranted by the facts known after such reasonable effort to obtain facts and after meeting the requirements of paragraph (3). These standards are satisfied when the reviewers with the knowledge they possessed at the time of the professional review, would reasonably believe that their actions would restrict incompetent behavior or would protect patients.

Overcoming HCQIA immunity. The HCQIA statute establishes a refutable presumption that professional review actions are presumed to meet the four HCQIA standards. However, this presumption can be overcome by a preponderance of the evidence. This means that to overcome the immunity that HCQIA afforded Blue Cross and Dr. White, Dr. Singh must demonstrate that a reasonable jury could find that Blue Cross and Dr. White failed to follow the HCQIA dictates in their peer review actions.

After a lengthy discussion of the role of the jury in HCQIA-based actions, the court compared actions for rights violations brought under HCQIA and those brought under 42 U.S.C. §1983, lawsuits against officials acting in their official capacity. Immunity under HCQIA was immunity from damages only, not immunity from suit as under Section 1983. Section 1983 suits are questions of law asking whether rights at issue were established; here no legal issue existed—only medical issues that could be evaluated by jurors with, if needed, medical experts as in medical malpractice cases.

In ruling against Dr. Singh, the court determined that his assertion that the district court's dismissal judgment deprived him of his right to a jury trial overlooked Congress's intention in adopting the objective standards for HCQIA immunity. The court reasoned that if there are no issues of material fact, if the evidence of reasonableness under HCQIA is so one-sided that a jury could not find that HCQIA standards were violated, the dismissal motion known as a summary judgement does no violence to an individual's right to a jury trial.

HCQIA immunity applied. The court reviewed the professional review actions, challenged by Dr. Singh, under the HCQIA standards. Professional review actions are statutorily defined as actions by a professional review body taken in the conduct of professional review activity based on an individual physician's conduct that could adversely affect the care of a patient and the privileges of the physician. Dr. Singh's extensive arguments that both the first and second audits did not meet the HCQIA immunity standards failed. The court reviewed each audit based on the factors required for HCQIA immunity to apply; namely (1) the reasonable belief that the actions were taken to further quality healthcare, (2) the adequacy of the fact finding, and (3) the adequacy of the notice and hearing procedures given to Dr. Singh.

This decision lends great support to the "rush to quality healthcare" in America today.

The court determined that no reasonable jury could deny Blue Cross's assertion that its professional review actions met the HCQIA standards for immunity. Therefore the court ruled that Blue Cross was immune from liability for the first and second audits. Also, immunity would be extended to Dr. White because HCQIA's protection extends to anyone participating in a peer review body with respect to actions arising out of that peer review.

HCQIA immunity scope. Since HCQIA immunity only covers liability for damages, defendants are not shielded from suit or other forms of review. The court then reviewed the dismissal motion on the merits. The contract, defamation, and all the other claims failed at the appellate level just as they had at the district court level. Therefore the district court's dismissal motion, previously granted to Blue Cross and Dr. White, was affirmed.

Decision's importance. This decision lends great support to the "rush to quality healthcare" in America today, as comprehensive peer review actions are critical in attaining and maintaining good healthcare. Insurers as well as healthcare professionals can be confident that if they follow HCQIA dictates, protection will be granted for their peer review activities and actions. This is of no small import given all the players, politics, and power struggles in healthcare institutions.

Both the CCH Healthcare Compliance Letter and CCH Healthcare Compliance Reporter covered the district court case. (See CCH Healthcare Compliance Letter, Vol. 4, Issue 21, Nov. 5, 2001, and CCH Healthcare Compliance Reporter, ¶305,225 (Oct. 4, 2001). ■

Singh v. Blue Cross/Blue Shield of Massachusetts, Inc., 1st Cir., No. 01-2586, Aug. 27, 2002, ¶301,460