CCH Healthcare Compliance LETTER

Volume 6, Issue 5 www.cchgroup.com March 17, 2003

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

Extension on HIPAA Privacy Rule unlikely

by Catherine Hubbard, Contributing Editor

There is little chance Congress will extend the April 14, 2003 Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule compliance date, according to experts who spoke at a HIPAA conference in early February. Kirk J. Nahra, with Wiley Rein & Fielding predicted, there "won't be a change" in the date adding, "it would take something cataclysmic for there to be a change."

William R. Braithwaite, M.D., with PricewaterhouseCoopers, Washington, D.C. noted that Congress was unable to write the Privacy Rule, making it extremely unlikely they would agree to an extension. "There won't be an extension," he predicted.

Even though time is running out, providers should not worry about strict penalties for failing to comply perfectly with the rule, Nahra said. As long as providers act in a reasonable manner to protect patient privacy, there is little chance that the Department of Health and Human Services (HHS) will clamp down, he said: "[y]ou do anything remotely reasonable and you will not go to jail for this," even if the Office of Civil Rights (OCR) does determine there has been a violation of privacy. He noted that many large providers will spend millions to avoid the $25,000 penalty. Although criminal penalties are steeper—up to $250,000 and 10 years in prison—providers that act in due diligence are highly unlikely to receive these fines, he said.

In addition, there is no penalty if the provider is unaware of the violation and if by exercising reasonable diligence the entity would not have known of the violation, said Nahra. Furthermore, there is no penalty if the violation is due to reasonable cause and not to willful neglect, if the problem is corrected. The OCR's approach is to increase compliance through education, cooperation and negotiation, said Nahra: "[t]hey're not looking to punish."

"The enforcement procedure likely will not be so bad after all," said Alan S. Goldberg, Esq., a partner with, Goulston & Storrs, Washington, D.C. "Civil penalties under HIPAA should be imposed leniently and in a way that will encourage compliance and not make covered entities feel as if they are being persecuted for inadvertent violations," he added.

Compliance Challenges. Nevertheless, there are some tricky situations to look out for, Nahra warned. For instance, the minimum necessary standard has been confusing to providers, he said. The standard means that when using or disclosing protected health information (PHI) or when requesting such information from another covered entity, the covered entity must make all reasonable efforts

to limit PHI to the minimum amount necessary to accomplish the intended use or disclosure. However, providers do not have to take excessive precautions to protect privacy, such as tearing down hospital walls to provide all patients private rooms, Nahra said. A more reasonable approach is to put screens between beds, he said.

Another thorny area of the rule concerns the right of members to request confidential communications, said Nahra. For example, if a wife seeks a pregnancy test but tells the doctor's office that she fears that if her husband finds out about the visit he will harm her, then the provider must be extremely careful in handling the situation, he said. While general protocol calls for the provider to send the bill to the named insured—the husband in this case—doing so could place the wife in harm, he said. "That's got to be handled at a high level, very, very carefully," he cautioned. The provider should set up a system so that if it receives such a request, "bells and whistles go off," he said.

A difficult situation also arises when a person requests their spouse's PHI with the intent of using the information against him or her in court during a custody battle, said Nahra. Although there are a low percentage of problems like these, the risk is high when problems occur.

Litigation Concerns. Providers should also be concerned about private litigation, Nahra said. In addition, he said, pressure and adverse publicity will be important concerns. "Publicity will drive compliance," adding: "[t]hat's going to be the biggest concern for covered entities."

"Don't surprise the patient," said Braithwaite. A good rule of thumb for avoiding lawsuits is whether the patient knows how his or her PHI is being used. "It's a surprised patient that goes to a lawyer," he said. Although the new system will require staff training and will unsettle providers for awhile, it "will become part of the way we do business" and "pretty soon it won't be a big deal," Braithwaite commented. "But before April 14, it will be a big deal."

CCH Washington Bureau, February 2003

Intrusion into clinic databases raises HIPAA considerations

by Raio G. Krishnayya, J.D.

In May of 2002, a Veteran's Administration (VA) hospital in Indianapolis, Indiana reported what was deemed by an Indiana Congressman, a "breach in security." *See Sensitive VA medical and credit info found on $10 computers*, CCH Healthcare Compliance Letter, Vol. 5, Issue 11, June 10, 2002. In the case of the VA hospital, the "breach" occurred when investigative reporters discovered protected health information on the hard drives of computers discarded by the hospital.

History appears to have repeated itself. A recent article by the Indianapolis Star reported that the Indiana University (IU) Center for Sleep Disorders experienced extensive intrusion into its computer records by a computer hacker.

IU's Chief Information Officer, Vince Sheehan, noted that the hacker would have had access to approximately 7000 patient records including names, dates of birth, social security numbers, and addresses. The records span fourteen years of patient data gathered by the clinic, however, University officials are fairly certain that the hacker did not have access to medical treatment records of the patients. In addition, IU spokespersons indicated that they did not have evidence that the hacker either downloaded or stole any of the information. However, the University is urging patients whose data was stored on these records to maintain close surveillance of the use of their information including financial information.

This does not mark the first instance of a breach of IU's systems. The Indianapolis Star reported that this breach marked the third intrusion in a two-year period. According to Sheehan, "[o]ur system hosts 50,000 computers that send over a billion e-mail transactions each year."

Such staggering statistics indicate that almost any corporation or organization, including and especially healthcare providers, are far more susceptible to computer breaches than one would normally consider—the kinds of breaches that the Health Insurance Portability and Accountability's (HIPAA) Privacy and Security Rules were designed to address.

Liability. The IU scenario raises the issue; what would be the liability under HIPAA? Looming are the HIPAA associated penalties, which allow for both criminal and civil penalties. Civil penalties under HIPAA include $100 per violation up to a maximum of $25,000 per calendar year. Granted that up to $25,000 does not seem overly burdensome when compared to large judgments under the

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., L.C.S.W.

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

Designer
Jason Wommack

Comments from readers are welcome and should be directed to Jeff Reinholtz at REINHOLJ@CCH.COM, Tel. 847-267-7316, Fax 847-267-2514. Customer service inquiries should be directed to 800-449-9525.

CCH Healthcare Compliance Letter is published 24 times a year by CCH INCORPORATED, 4025 W. Peterson Avenue, Chicago, IL, 60646. Subscription rate is $305 per year. First-class postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: SEND ADDRESS CHANGES TO *CCH Healthcare Compliance Letter*, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A.

False Claims Act, for example, which can range in the millions of dollars. However, a closer reading indicates that this amount is **per violation**.

In the context of the IU case, and assuming that IU had been found to violate the Privacy Rule, there are three possibilities under the term **per violation**. Under the first possibility, the hacker's intrusion into the records could be treated as one violation and thus would place IU in jeopardy of only paying the $25,000. A second possibility is that each intrusion by the hacker could be considered mutually exclusive violations. However, under this scenario, a court could consider these as concurrent events for damages purposes and as such treat the breaches as only one breach. A provider would be only responsible for the $25,000. The last scenario is the worst case.

In the IU case, the breach was discovered in January of 2003 and while the records indicate that the breach was a one-time occurrence, it would be difficult to determine how many times a breach may have occurred. Consider a scenario where IU had been subject to repeated breaches. The worst-case possibility presumes that each incident equals one violation. Furthermore, a court that refuses to consider these as concurrent events could treat the events as consecutive breaches thus, the provider would be liable for $25,000 times the number of times a breach could be shown.

The worst case presumes, however, that the provider was extremely negligent in terms of maintaining even basic protections. Furthermore, under such recklessness on the part of the provider, the issue may be less about civil penalties and more about criminal penalties.

The key to the HIPAA criminal penalties is to realize that a "knowledge" element is included. The relevant provision states:

> A person who knowingly and in violation of this part (1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall be punished as [follows]...(1) be fined not more than $50,000, imprisoned not more than 1 year, or both; (2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both....

In the IU case then, the government would have to show that the University "knowingly" allowed the hacker to violate one of the HIPAA standards (i.e. the Privacy Rule). As a practical matter, this is a somewhat high standard to demonstrate since anything short of willful disregard of **any** privacy or security measures would be the kind of evidence needed to secure a conviction under HIPAA.

Equally important, HIPAA compliance officers must realize that relevant to any case is whether the information released was protected health information. The IU case reveals an interesting dichotomy because on the one hand, the information that could have been compromised was **not** protected health information but rather identification information. On the other hand, the hacker's intrusion occurred into the records of the sleep clinic thus, there is an argument that protected health information could have been compromised. In other words, the breach into identification materials—thereby giving access to treatment records—could have been a compromise of information contemplated by HIPAA.

In either case, what is clear is that investigators will carefully look to the privacy and security practices of healthcare entities to eventually determine if HIPAA liability should be imposed. Scenarios such as the one presented by the IU case indicate that no system is 100 percent impervious to hackers and that such breaches raise many questions yet to be answered under HIPAA.

A copy of the Indianapolis Star article can be found at http://www.indystar.com/print/articles/2/026103-7472-009.html. The article may also be access through the hipaadivsory.com website at http://www.hipaadvisory.com/news/index.cfm#0304is. ■

CCH Chicago Bureau, March 1, 2003

On The Front Lines

Fearing a revolution: Genetics and the Privacy Rule (part II of II)

by Gordon R. Shea, J.D.

From Part I: *Despite recent guidance issued by HHS's Office of Civil Rights (OCR) stating that "genetic information is health information protected by the Privacy Rule" of the Health Insurance Portability and Accountability Act (HIPAA), this did not necessarily make it so. While § 701 of HIPAA does address genetic information, it does not directly speak to the privacy of such information.*

Norman-Bloodsaw. The plaintiffs in *Norman-Bloodsaw* maintained that they had no knowledge that samples from employer-required medical tests were being used to screen employees for syphilis, sickle cell problems, or pregnancy. Therefore the testing "occurred without their knowledge or consent," as well as "without any subsequent notification that the tests had been conducted." The plaintiffs also alleged that prohibited race discrimination was inherent in the tests since the only employees screened for sickle cell anemia were African-American. Lastly, the plaintiffs charged that the laboratory "failed to provide safeguards to prevent the dissemination of the test results." The plaintiffs also maintained that by requiring these tests and handling them as they did, employer-defendant Berkeley Laboratories violated their federal and state (California) constitutional right to privacy. Some of the plaintiffs contended that 42 U.S.C. Title VII had been violated because African-American employees had been singled out for sickle cell trait testing, and women had been singled out by pregnancy testing.

The case eventually turned on procedural matters. A district court disposed of the plaintiffs' contentions on summary judgment; the specific matter to be decided by the U.S. Court of Appeals for the Ninth Circuit was whether the lower court erred in its approach to the case.

Ultimately, the Ninth Circuit reversed the lower court in part, although that part was the heart of the genetics-based case. The court began by noting that the record in the case "strongly suggests that plaintiffs' submission to the exam did not serve to afford them notice of the particular testing involved." Moving to the substance of the plaintiffs' claims, the court then stated that the "constitutionally protected privacy interest in avoiding disclosure of personal matters clearly encompasses medical information and its confidentiality." Coming down particularly hard on defendant Lawrence Berkeley Labs with regard to the federal constitutional claims against it, the court said that:

> [I]t goes without saying that the *most basic* violation possible involves the performance of unauthorized tests - that is, the non-consensual retrieval of previously unrevealed medical information that may be unknown even to plaintiffs. These tests may also be viewed as searches in violation of Fourth Amendment rights that require Fourth Amendment scrutiny. The tests at issue in this case thus implicate rights protected under both the Fourth Amendment and the Due Process Clause of the Fifth or Fourteenth Amendments. ...One can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health or genetic make-up.... Furthermore, the facts revealed by the tests are highly sensitive, even relative to other medical information. With respect to the testing of plaintiffs for syphilis and pregnancy, it is well established in this circuit "that the Constitution prohibits unregulated, unrestrained employer inquiries into personal sexual matters that have no bearing on job performance."

The Ninth Circuit then flatly stated that the "plaintiffs' Title VII claims fall neatly into a Title VII framework," particularly in alleging that female and African-American employees were "singled out for nonconsensual testing:"

> In this case, the term or condition for black employees was undergoing a test for sickle cell trait; for women it was undergoing a test for pregnancy. It is not disputed that the preplacement exams were, literally, a condition of employment: the offers of employment stated this explicitly. Thus, the employment of women and blacks at Lawrence was conditioned in part on allegedly unconstitutional invasions of privacy to which white and/or male employees were not subjected. ... The unauthorized obtaining of sensitive medical information on the basis of race or sex would in itself constitute an "adverse effect," or injury, under Title VII.

This overall result—that the plaintiffs' genetic testing claims raised definite constitutional concerns and fit "neatly" into a tried-and-true Title VII discrimination framework—was fine for many of the particular plaintiffs. However, particularly since the Ninth Circuit's decision was ultimately focused on the nar-

row matter of whether a lower court had erred, what the Ninth Circuit's opinion did *not* do was establish broad legal principles regarding genetic privacy. Non-minority men, women subjected to genetic testing for non-sex-specific conditions, and African-Americans tested for anything not related to sickle-cell anemia— any of these groups generally—could not place much reliance on the *Norman-Bloodsaw* opinion.

The HIPAA frontier. Despite the fact that *Norman-Bloodsaw* may seem highly fact-specific, two key factual concepts suggest broader implications. Those concepts were notice and consent.

In particular, the word "consent" (or variations on it, such as "consenting" or "consented") appeared in the Ninth Circuit's *Norman-Bloodsaw* opinion no fewer than 13 times. Early in its discussion of the case, for example, the Ninth Circuit noted that the record in the case contained "considerable evidence "that the manner in which the tests were performed was inconsistent with sound medical practice" in large part because "the performance of such tests without explicit *notice and informed consent* violates prevailing medical standards" (emphasis supplied). A "significant difference," the court later said, exists between responding to medical questions,

> on the basis of what you know about your health and consenting to let someone else investigate the most intimate aspects of your life. ... Plaintiffs could reasonably have expected Lawrence to *seek their consent* before running any tests not usually performed in an occupational health exam - particularly tests for intimate medical conditions bearing no relationship to their responsibilities or working conditions as clerical employees. The mere fact that an employee has given a blood or urine sample does not provide *notice* that an employer will perform any and all tests on that specimen that it desires - no matter how invasive - particularly where, as here, the employer has yet to offer a valid reason for the testing. ... That one has *consented* to a general medical examination does not abolish one's privacy right not to be tested for intimate, personal matters involving one's health....

HIPAA Privacy Rule relation. Until recently, HIPAA'S Privacy Rule contained a prior consent requirement that was so important as to be really the Rule's *sine qua non*. This version of the Rule, which was the version promulgated during the Clinton administration, would likely have meant that any employee or prospective employee would have been required, by the government, to give his or her written consent before undergoing the kinds of genetic screenings and tests that the employer in the *Norman-Bloodsaw* case demanded. Note that while the employer, Lawrence Berkeley Laboratories, would probably not be considered a traditional "covered entity" under HIPAA, it might well be subject to the law nonetheless as a "hybrid entity" that engages in a significant healthcare function by virtue of its practice of genetically testing employees.

Under Bush administration-era changes to the Privacy Rule, however, the notion of consent (prior or otherwise) has been all but abandoned. It was replaced with a "good faith" requirement that healthcare entities advise individuals of the entities' privacy policies, and then leave such individuals free to go to another institution if they do not approve of those policies.

Compared to the never-finalized Clinton-era approach to the Privacy Rule, the Bush approach is a far less comfortable fit with the still-nascent and developing law as embodied in the *Norman-Bloodsaw* decision. While *Norman-Bloodsaw* is only one decision from the single, oft-criticized Ninth Circuit, the practical effect of the divide between that decision and the now-finalized HIPAA Privacy Rule should not be gainsaid. Where once there was a developing symmetry between genetic privacy policies being developed in Washington and those being vetted by at least one major court, there is now disconnect.

Philosophy by rote? The writer Ralph Waldo Emerson once warned that, too often, "[w]e wish to learn philosophy by rote, and play at heroism." But, he added,

> the wiser God says, Take the shame, the poverty, and the penal solitude, that belong to truth-speaking. Try the rough water as well as the smooth. Rough water can teach lessons worth knowing.... Fear not a revolution which will constrain you to live five years in one. Don't be so tender at making an enemy now and then."

Though the Department of Health and Human Services has shown little tenderness in making enemies when it comes to tinkering with HIPAA's Privacy Rule, the final Rule seems to have been crafted by those who did indeed fear the revolution that earlier drafts of the Rule represented. The resulting Final Privacy Rule is somewhat less bureaucratic than earlier versions of the Rule but it is a rule that has diverged from at least some emerging law. It therefore may ultimately yield greater legal uncertainty in the area of genetics than would otherwise have been the case.

Gordon R. Shea is a licensed attorney and a CCH Healthcare Compliance Law Analyst and Editor. Several of his HIPAA writings are collected on the website www.hipaa.chh.com. For more information, Mr. Shea may be contacted at CCH INCORPORATED, 2700 Lake Cook Road, Riverwoods, Illinois 60015, Phone: (847) 267-2812, E-mail: sheag@cch.com.

1 http://www.hhs.gov/ocr/hipaa/guidelines/guidanceallsections.pdf
2 *Norman-Bloodsaw v. Lawrence Berkeley Lab.,* 135 F.3d 1260, 1264, 9th Cir. Ct. of Appeals (1998).
3 Id.
4 Id. at 1265.
5 Id.At 1267.
6 Id.At 1269.
7 Id. (emphasis supplied).
8 Id.At 1272.
9 Id.At 1268.
10 http://www.emersoncentral.com/culture.htm

Teaching hospitals get lesson in fraud

by Gordon R. Shea, J.D.

A once-unpromising False Claims Act (FCA) action in Missouri has turned into a potentially precedent-setting case for teaching hospitals and their residency programs.

Residents or physicians? The case, *U.S. ex. rel. Schuhardt v. Washington University*, began as a *qui tam* action by two coding workers at the teaching hospital associated with Washington University. One of the workers in particular, Schuhardt, said she repeatedly complained to her supervisor about the hospital's allegedly "fraudulent" billing of surgical procedures by attending physicians to the federal government. In particular, Schuhardt alleged that the hospital had billed the following procedures performed by physicians, claiming to have been present during the procedures, who, in fact, were not:

- Pre- and post- operative care
- Surgeries
- Surgical consultations among doctors
- Bedside procedures
- Emergency room procedures
- Night and weekend services
- Wound-healing clinic services

Schuhardt alleged that these actions were often performed by residents, fellows, and nurses, and not by attending physicians. She also alleged that attending physicians were frequently failing to even supervise the procedures. According to Schuhardt, her attempts to stop this fraudulent billing resulted in employment harassment and her eventual termination. When she later filed a *qui tam* action against the hospital, the government demurred from joining it saying that Schuhardt and her fellow plaintiff had not demonstrated their fraud claims with the requisite particularity.

After an extensive review of the legislative and other history surrounding the Medicare Act, Judge Carol E. Jackson concluded, for the Eastern District of Missouri federal court, that there was a split in time concerning the issue: until "June of 1996, Medicare required a teaching physician to be present, for both surgical services and pre- and post- operative care, in order to receive reimbursement" under Medicare. "Furthermore," according to her opinion, "it is this Court's interpretation of the regulations in effect from July 1, 1996 to present, that if the teaching physician decided that neither pre-nor post-operative services were 'key' portions of the billable service, then those services could be performed by a resident without the need for a teaching physician's physical presence during the service and still be eligible for reimbursement under" Medicare.

1967-95. Judge Jackson began by noting, that in August 1967, the then-Bureau of Health Insurance (now known as CMS) issued regulations that "were somewhat vague as to the presence requirement for pre- or post-operative care," in that they stated that only some "personal and identifiable direction was needed to apply for reimbursement." Two years later, the Bureau issued guidance in which, Judge Jackson said, it was "obvious" that the Bureau interpreted Medicare laws so as "to require a physician to be personally present at the time of surgical services and pre- and post- operative" procedures. "This message became even clearer," according to Judge Jackson, "in later legislative history surrounding reimbursement for teaching physicians," starting with 1980 changes to the law. In 1995, however, Jackson wrote that CMS "confused" its guidelines by sending out a letter saying that CMS had not issued a final rule on the physical presence requirement, and by later issuing a preamble to teaching hospital rules in which the agency called its policies "`vague, perhaps, necessarily, on the matter of presence of the physician during other occasions of inpatient service.'"

Finally, in 1997, CMS's general counsel issued an opinion letter that seemed to return to the pre-1995 interpretation of the relevant Medicare rules. The federal court ultimately relied on this latter interpretation. It endorsed the view that the physical presence of physicians was required for reimbursement between 1967 and 1996 as CMS's last word on the matter indicating that this view was also a better fit with "common sense" and the "history" of the subject.

1995-Present. As for whether or not there was a physical presence requirement for reimbursement-receiving teaching physicians after 1995, Judge Jackson said "the Court can only look to the regulations themselves for assistance in interpreting such a requirement." The most relevant regulation in the Court's view was 42 CFR § 415.172, which "states that a physician fee schedule payment will be made only if a teaching physician is present during the key portion of any service or procedure for which payment is" desired. The question of determining what portion of a medical procedure is "key," the court said, is best determined by teaching physicians themselves in each individual circumstance.

Other issues & implications. Another issue in the case was the issue of whether Schuhardt and the other plaintiffs pled their case with sufficient "particularity," or specificity. This has recently been a "hot topic," given that increasing numbers of FCA cases seem to have failed on this basis (see *FCA claims denied for failure to "state with particularity," CCH Healthcare Compliance Letter, Vol. 5 No. 15, Aug. 5, 2002*). Here, Judge Jackson wrote that Schuhardt sufficiently detailed the fraudulent "who, where, and when." "No longer is plaintiffs' complaint based on just 'information and belief," Jackson said. "Plaintiffs have named specific doctors, and have identified specific dates and services supporting their allegations of improper Medicare billings."

Schuhardt illustrates the increasing scrutiny that academic medical programs are coming under regarding allegedly fraudulent conduct. In another recent example, just this month Northwestern University agreed to pay the government $5.5 million to settle allegations that the school violated the FCA in connection with federal medical research grants. Following this settlement, Assistant Attorney General Robert D. McCallum, Jr., of the Department of Justice Civil Division, noted the increased focus on academic institutions and spoke of "the importance to the United States of ensuring that universities and other institutions make proper use of federal research funds." ■

U.S. ex. rel. Schuhardt v. Washington University, No. 4:99-CV-1202 CEJ, E.D.Mo., Aug. 20, 2002, ¶301,466

No liability for hospital but JDs pay in immigration scheme

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

Recruiting foreign physicians can be a legal minefield despite a health system's best efforts. This was the lesson learned by an Iowa health system, Trinity Health Systems, Inc., and its physician group, Trimark Physicians Group, in its effort to recruit a Canadian physician, Gregory DePape, for a family practice position. Although both entities avoided liability when Dr. DePape sued them, the immigration law firm involved paid damages stemming from its legal malpractice.

Contract but no visa. Dr. DePape, the health system and the physician group had signed a five-year contract for a family physician. All the parties had high hopes that it would be a permanent position. Trinity and Trimark hired Blumenfeld, a Missouri immigration firm, to handle the immigration process. Perhaps Dr. DePape, Trinity and Trimark should have been leery of the immigration law firm when Blumenfeld instructed Dr. DePape to enter the United States on a specific day via the Peace Bridge in Buffalo, New York almost 3,000 miles away. Most notably, Blumenfeld had almost no contact with Dr. DePape and minimal contact with Trimark during this entire process.

After learning that he would be granted an Iowa medical license, a date was set for Dr. DePape's entry into the United States. Blumenfeld arranged for him to meet an attorney, formerly an immigration officer at the Peace Bridge, on the Canadian side of the bridge. There the attorney informed Dr. DePape, for the first time, that he could not enter as a family physician. Instead, the required entry letter from Trinity described him as a "physician consultant," a Blumenfeld-contrived position, under a temporary visa for Canadian and Mexican professionals called a TN. Unbeknownst to Dr. DePape this visa carried severe limitations on direct patient care. Blumenfeld indicated to Dr. DePape that he would be using a TN visa but never informed him that he could not enter the United States as a family physician.

Dr. DePape never entered the United States on the appointed day. The immigration officer did not believe that Dr. DePape sought entry to the United States to perform a community needs assessment as physician consultant and sent him back to Canada. After contacting Trimark, Dr. DePape was told to enter as a visitor, which also failed and resulted in the immigration officials interrogating him and searching his car.

Action against Trinity and Trimark. Dr. DePape, homeless and without a job, sued Trinity, Trimark and Blumenfeld. Dr. DePape's first argument against Trinity and Trimark—that they promised him legal entry into the United States—failed because the court viewed their mutual agreement as a goal and not a promise. Trimark had fulfilled the promises that it made to Dr. DePape; it retained an immigration firm and paid all legal fees.

In a separate argument against Trimark, Dr. DePape claimed that Trimark breached its contract with him. The court determined that Trimark was liable for nonperformance of the contract because Dr. DePape was never allowed to enter the United States. Because neither party could fulfill its duty of performance under the Employment Agreement, Trimark was relieved of its obligation to perform.

In his third count, Dr. DePape alleged that both Trinity and Trimark assumed a duty to obtain government permission to allow him to practice medicine in the United States and to make all the arrangements. The court ruled that: (1) there was no relationship between the parties that gave rise to a legal obligation to gain permission for Dr. DePape to practice medicine in the United States, and (2) if there had been a recovery, it would only be in a contract claim and not a tort claim.

The court further determined that it was readily apparent, early in the case, that Trinity and Trimark had no liability in this case. Therefore, the court stated that if Trinity and Trimark had requested sanctions under Rule 11 of the Federal Code of Civil Procedure, it would have granted them.

Legal malpractice claim. Dr. DePape amended his compliant on the eve of trial and added a legal malpractice claim against Blumenfeld. Dr. DePape successfully demonstrated that: (1) there was an attorney-client relationship which gave rise to a duty, (2) the attorney, either by an act or failure to act, violated or breached that duty, (3) the attorney's breach of that duty proximately caused injury to him, and (4) he sustained actual injury, loss or damage.

The strength of Dr. DePape's legal malpractice count was that Blumenfeld breached its duty by failing to communicate with him and failed to advise him of the severe limitations of the TN visa. The court found that Blumenfeld never explained the TN visa and sprung the illegal physician consultant-community health care needs assessment theory on him at the Peace Bridge. The court determined that damages should be awarded because Dr. DePape could have alternately pursued his career in Canada had he been properly informed of his immigration options but for the misrepresentations made by Blumenfeld.

Damages awarded. The court ordered Blumenfeld to pay damages based for Dr. DePape's lost income, $203,736.20, and emotional distress, $75,000. The court further stated that punitive damages could have been awarded had Dr. DePape pled sufficient facts.

Importance. Due to shortages in all types of healthcare professionals, more and more hospitals are turning to foreign countries to staff their facilities. This case presents an in-depth discussion of two visas, the H-1B visa and the TN visa, which is governed by the North American Free Trade Agreement.

Hospitals need to increase their knowledge about the immigration process and monitor outside consultants working on any project. Although both healthcare entities in this case, Trinity and Trimark, were absolved from any liability, they still incurred legal fees in addition to their personnel costs. ■

DePape v.Trinity Health Systems, Inc., No. C01-3043-MWB-Memorandum Opinion and Order Regarding Bench Trial on the Merits, N.D. of Iowa, Central Division, Jan. 20, 2003, ¶301,467

continued on page 8

IG: compliance critical to quality healthcare

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

According to the Department of Health and Human Service's, Inspector General, Janet Rehnquist, compliance professionals play a key role in the delivery of quality healthcare. In her presentation at the Sixth Annual National Congress on Health Care Compliance in Washington D. C., Rehnquist stated that effective compliance programs were critical in the face of the increased healthcare needs of an aging population. She emphasized that: (1) compliance professionals make a difference, (2) the Office of Inspector General (OIG) supports them, and that there was more work to be done. Rehnquist then addressed the government's success in enforcement, highlighting a report on outpatient procedures, and disclosed the OIG's future efforts in promoting healthcare compliance.

OIG enforcement initiatives. In a combined effort by OIG, the Federal Bureau of Investigation and the Department of Justice to combat healthcare fraud, the government has recouped 1.8 billion dollars in compliance-related judgments or settlements. Rehnquist cited the False Claims Act as a powerful tool in this fight against fraud and stated that the OIG will establish False Claims Centers in specific United States Attorneys' offices.

Reimbursement basis should change. In her address she also presented the OIG's recommendations based on a recent Office of Evaluation and Inspections report, "Payment for Procedures in Outpatient Departments and Ambulatory Surgical Centers," which found that reimbursement disparities for certain procedures resulted in additional Medicare payments of $1.1 billion dollars. In order to maximize government healthcare dollars, she recommended that Medicare reimbursement be service-based, not setting-based.

OIG's future plans. The Inspector General also stated that the OIG would continue to be proactive in its support of healthcare compliance efforts. Two new guidances will be issued: one for the ambulance industry, and in spring or summer 2003, one for the pharmaceutical industry.

Rehnquist also emphasized the OIG's goals for compliance programs and its future areas of review. The OIG wants compliance programs that are effective, values-based and emphasize corporate self-governance. Because compliance program effectiveness has not been measured, the OIG and the Centers for Medicare and Medicaid Services plan to develop such a tool.

The OIG has established potential risk areas that it intends to review. These potential risk areas are: (1) medical necessity of services, (2) upgrading of services, (3) consultants promoting revenue-enhancing schemes, and (4) the independence of Independent Review Organizations.

Importance. Throughout her presentation, Rehnquist continually emphasized quality and its importance in compliance programs. Additional proof that the government is serious about quality has been provided by the issuance of a final rule, effective March 25, 2003, which requires that hospitals develop and maintain a quality assessment and performance improvement program. This Quality Assessment and Performance Improvement Condition of Participation focuses on the actual care delivered to patients, the performance of the hospital or health system as an organization, and the impact of treatment on the health status of its patients.

Compliance professionals need to act on the words of the Inspector General and the power behind government regulations to improve and expand their compliance programs. The government has said that quality initiatives must be an integral part of any compliance program. Also, the government has demonstrated that it expects compliance programs to expand beyond mere adherence to requirements and instead, be values-based. Compliance professionals are pivotal to achieving this expansion. The OIG has stated that it stands behind them in their efforts. ■

OIG-Payment for Procedures in Outpatient Departments and Ambulatory Surgical Centers, OEI-05-00-00340, Feb. 6, 3003, ¶154,109; CMS-Medicare and Medicaid Programs: Hospital Conditions of Participation: Quality Assessment and Performance Improvement, 68 FR 3435, ¶157,004