Healthcare Risk Management®

Celebrating our 27th year as your first source of risk management information

THOMSON
AMERICAN HEALTH CONSULTANTS

IN THIS ISSUE

Financial Disclosure:
Editor Greg Freeman, Editorial Group Head Lee Landenberger, and Nurse Planner Maureen Archambault report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study.

SEPTEMBER 2005
VOL. 27, NO. 9 • (pages 97-108)

Rise in medmal premiums prompts dispute over potential of profiteering

But real reason may be more complicated, analysts say

Malpractice insurers are stinging from charges of profiteering from insurance premiums by new data showing costs rising dramatically as claims drop. Some of this information may make risk managers wonder if they have been overcharged by insurers who say they are barely scraping by.

But before you pick up the phone and give your insurance broker an earful, you might want to hear the other side of the story.

The data in a recent study are misleading, say some prominent insurance industry players, and the charges of profiteering come from an outfit that calls itself a consumer advocate group but is primarily concerned with opposing tort reform.

The claims in the recent report will be troubling to risk managers who struggle every year to get the best malpractice premiums and still see costs rise. There may be reason to question your insurance provider more closely and to understand the issues on a deeper level, but *Healthcare Risk Management* editorial advisory board member **R. Stephen Trosty**, JD, MHA, CPHRM, director of risk management for American Physicians Assurance Corp. in East Lansing, MI, says the claims of profiteering are unfounded.

"This is not an accurate and valid study, and I'm afraid it's going to upset people unnecessarily," says Trosty, whose employer is criticized in the report. "It does not take into account the realities of the industry."

Group has ties to Michael Moore, Erin Brockovich

The key conclusion in the report, "Falling Claims and Rising Premiums in the Medical Malpractice Insurance Industry," is that medical malpractice insurance rates for doctors have skyrocketed in recent years even though claim payments are down.

"These findings suggest that doctors have been price-gouged for several

years as insurance industry profits have ballooned to unprecedented levels," the report says. It cites AIG, which is under investigation by state and federal authorities for its business practices, and Health Care Indemnity Inc., a subsidiary of HCA, the largest for-profit hospital chain, as among the worst offenders.

The study was prepared by former Missouri Insurance Commissioner **Jay Angoff** and was commissioned by the Center for Justice & Democracy (CJ&D) in New York City and coreleased by several other advocacy organizations, including Alliance for Justice, Consumer Federation of America, Public Citizen, USAction, and U.S. PIRG.

CJ&D describes itself as a group "that works to educate the public about the importance of the civil justice system and the dangers of so-called 'tort reforms.' CJ&D fights to protect the right to trial by jury and an independent judiciary for all Americans." The CJ&D web site (www.centerjd.org) offers a promotional video titled "Trial Lawyers, The Last Line of Defense."

In addition to a host of law professors, two of the most prominent members of the CJ&D Board of Advisors are filmmaker Michael Moore and legal activist Erin Brockovich, whose story was told in the movie starring Julia Roberts.

Based on info supplied under oath

Trosty notes that CJ&D is clearly opposed to tort reform, making it a friend of trial attorneys even if there is no formal association with them.

"We're going to see more of these studies, not fewer, and risk managers need to look closely at who is doing the study," he says. "If they are just fronting for trial lawyers or another group, they already have a preset message and there's the old adage that you can make data fit any message you want to deliver."

But there is no denying that some of the group's conclusions are intriguing and potentially troubling for risk managers.

The CJ&D report is an analysis of the 2000-2004 performance of each of the 15 largest AM Best-rated malpractice insurers in the United States. The conclusions are based upon an examination, for the first time, of statements supplied under oath to state insurance departments by the nation's top medical malpractice insurers. The report charges that the insurance industry has been overcharging providers significantly despite the fact that their claims payments, in real terms, have dropped since 2000.

CJ&D claims that contrary to the impression they have given health care providers and the general public, the losses that medical malpractice insurers predict they will pay in the future — the insurers' purported basis for current rate hikes — are down as well. Trosty says the report is wrong on that count. **(See p. 101 for more details of the report's conclusions.)**

Group: Numbers don't jibe with industry claims

Angoff says the leading malpractice insurers' Annual Statements indicate that they have been raising their premiums even though both their actual claims payments and their projected future claims payments have been falling.

Healthcare Risk Management® (ISSN 1081-6534), including **HRM Legal Review & Commentary**™, is published monthly by Thomson American Health Consultants, 3525 Piedmont Road, Building Six, Suite 400, Atlanta, GA 30305. Telephone: (404) 262-7436. Periodicals postage paid at Atlanta, GA 30304. POSTMASTER: Send address changes to **Healthcare Risk Management**®, P.O. Box 740059, Atlanta, GA 30374.

Subscriber Information

Customer Service: (800) 688-2421 or fax (800) 284-3291, (ahc.customerservice@thomson.com). Hours of operation: 8:30 a.m.-6 p.m. Monday-Thursday; 8:30 a.m.-4:30 p.m. Friday.

Subscription rates: U.S.A., one year (12 issues), $519. Outside U.S., add $30 per year, total prepaid in U.S. funds. For approximately 18 CE nursing contact hours, $545. Discounts are available for multiple subscriptions. For pricing information, call Steve Vance at (404) 262-5511. Missing issues will be fulfilled by customer service free of charge when contacted within one month of the missing issue date. **Back issues**, when available, are $87 each. (GST registration number R128870672.)

Healthcare Risk Management is approved for 18 nursing contact hours. Thomson American Health Consultants is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation. Provider approved by the California Board of Registered Nursing, Provider Number CEP 10864, for approximately 18 contact hours.

Editor: **Greg Freeman**, (770) 998-8455.
Vice President/Group Publisher: **Brenda Mooney**, (404) 262-5403, (brenda.mooney@thomson.com).
Editorial Group Head: **Lee Landenberger**, (404) 262-5483, (lee.landenberger@thomson.com).
Senior Production Editor: **Nancy McCreary**.

Editorial Questions

For questions or comments, call **Greg Freeman**, (770) 998-8455.

"The Annual Statement data thus prove that doctors have been overcharged during the last several years," Angoff says. "Those overcharges are obviously bad news for doctors, but they have resulted in good news for investors in the leading pure malpractice insurance stocks, which have doubled during the last three years while the stock market, as a whole, has remained flat."

Joanne Doroshow, executive director of CJ&D, says no amount of explanation from the insurance industry can counter the cold, hard facts in the report.

"To put it bluntly, if you look at what the insurance companies say about why they raise premiums, and then look at the data in this report, the numbers just don't add up," she says. "The facts are very simple: Medical malpractice payouts are down yet insurance companies have significantly increased premiums. This shows that the entire campaign to limit liability for doctors over the last several years by capping compensation to injured patients has been a fraud, and that based on these data, insurers must know that it has been a fraud."

Report raises concern about overpricing

Two state attorneys general and one state insurance commissioner have spoken out in response to the report, strongly condemning the actions by insurers to dramatically raise insurance rates for doctors while claims are dropping.

In a written statement, Connecticut Attorney General **Richard Blumenthal**, JD, said, "The numbers underscore the need for much tougher, more aggressive oversight to prevent and punish profiteering. Federal and state regulators should thoroughly scrutinize recent rate increases and take appropriate corrective action."

Missouri Attorney General **Jay Nixon**, JD, said "the data in the Annual Statements filed under oath with state insurance departments, which this report discloses, call into question much of what the medical malpractice insurance industry has been saying publicly during the past several years. There is no excuse for malpractice insurers doubling their rates while their claims payments decrease."

Michigan Office of Financial and Insurance Services Commissioner **Linda A. Watters** said, "We are definitely disturbed by the numbers in this report, which offers evidence that doctors may be paying excessive premiums. In the market competition study that we recently issued, we considered loss ratios below 50% as patently excessive. If these carriers truly have loss ratios that are this low and yet they are still increasing rates, one has to wonder if they're gouging."

PIAA says study intentionally misleads

Nonsense, says **Lawrence Smarr**, president of the Physician Insurers Association of America, the trade group that represents some of the biggest insurers. He says Angoff has long argued that insurance industry greed is the primary cause of rising premiums, and he charges that Angoff misuses data to prove his point.

In particular, Smarr points to Angoff's claim that between 2000 and 2004, "the amount the major medical malpractice insurers have collected in premiums has more than doubled, while their claims payouts have remained essentially flat."

"This is, of course, not true," he says. "The methodology he uses to arrive at this predetermined and erroneous conclusion is intentionally misleading and does not comport with widely accepted analytical standards."

If the conclusions in the report were true, Smarr says, the medmal industry would be thriving as it overcharged its customers and put the money in the bank. The truth, he notes, is that medmal insurers have been going out of

business in record numbers recently.

Smarr offers this list of what he calls major methodological flaws in the study that render the conclusions useless:

1. The study purposely excludes up to one-half of all insurer's costs.

Angoff's analysis inexplicably fails to take into account both allocated loss adjustment expenses (defense costs) and underwriting expenses (operating costs) paid or incurred, he says. These expenses together can equal the actual claim amounts paid out by an insurer and are directly related to the insuring and paying of claims, he adds.

2. The analysis compares apples to oranges in terms of time frames for claims.

Smarr says Angoff compares premiums written in a calendar year to claim payments made in the same year. While this would seem on the surface to make sense, it is actually not correct, he says. Medical liability is a "long-tail" line of insurance, and it usually takes between four and five years for a medical incident to work its way through the claim and adjudication/settlement process. Therefore, the premiums collected in any given year have absolutely nothing to do with the payments made in that same year (for which premiums were paid, on average, four or five years earlier). No legitimate actuary would ever make this kind of comparison, Smarr says.

Trosty explains further that the typical medmal case can take five to eight years for resolution, and so it doesn't make sense to compare this year's premiums to this year's claims. Juries are returning larger verdicts, he notes, so insurers must plan accordingly.

"What a company is paying out today is based on a premium that was probably paid five, six, seven years ago, at the rate providers were paying back then," Trosty says. "So you can't simply look at premiums today and claims today."

3. Angoff uses incorrect and misleading surplus calculation.

Angoff says that insurers have accumulated "record amounts" of surplus, but Smarr says he then cherry-picks which data-years to use in his calculation. He uses only the last three years, 2002-2004, because those years deviate from the surplus-consuming trend of the industry's past.

4. Risk-based capital smoke and mirrors mislead.

Smarr says Angoff inappropriately uses the National Association of Insurance Commissioners' (NAIC) risk-based capital standards to claim that insurers have more than adequate surplus. The NAIC however, states that insurers should seek to maintain surplus levels above the required minimum.

5. The analysis purposely leaves out the largest U.S. medmal insurance company.

Smarr charges that Angoff did this because the premium and cost data from the largest company, Medical Liability Mutual Insurance Co., would have thrown off his calculations and made his conclusions harder to reach.

Industry trying to catch up after deficit

Trosty suggests that risk managers should use the CJ&D study as an opportunity to more fully understand why they pay the premiums they do. Sit down with your insurance provider and ask for a thorough explanation of how the premium is priced, he says, with an eye beyond those factors unique to your own organization. A good discussion may put some fears to rest and it also will arm you in case your boss comes down the hall and asks why you let the insurance rip you off with high premiums.

Trosty notes that the insurance industry still is trying to catch up after years of charging premiums that were too low, based on claims, and that is why so many insurers have gone out of business or stopped offering medmal in some markets.

"A significant number of insurers went belly up in the last five years, and a large reason for that is that they were not charging adequate premiums," he says. "There was so much competition that everyone was trying to undercut each other. But that caught up to some companies and the dollars weren't there to pay off the claims, and they went bankrupt."

Trosty also points out that in most cases the insurance companies cannot just raise their premiums as much as they want. Rather, most states require the insurer to submit the proposed increases for approval, with proof that the increase is justified by actual claims payout and the company's surplus. Insurers are required to hold a certain surplus in reserve to account for any future increases in expenses.

"After companies started going out of business, state insurance departments started looking more closely at surpluses and found that some companies did not have enough in reserves to cover future claims," Trosty says. "So part of what we've been seeing is a correction of that

problem. That effort to improve reserves has been going on for years, and that is part of the increase we've seen in premiums."

The insurance industry is, by its nature, dependent on predicting the future, Trosty says. Charging premiums based on today's statistics is never enough, because the company must have the money in *future* dollars to pay claims, and those claims may be higher than they are today. Jury verdicts are increasing in both severity and frequency, he notes, so insurers must plan for larger payouts in the future.

"If premiums only increased literally by the amount of today's losses, in 10 or 15 years you'd have no medical malpractice insurance companies in existence," he says. "Future losses and payouts are not going to be what they are today. The money you pay in premiums is not to pay today's claims, but rather it's to pay claims five or six years from now when we know statistically that claims will be higher." ■

Report suggests claims are falling as rates keep rising

These are the key findings in the recent report from the Center for Justice & Democracy in New York City:

• **Actual payouts.** Over the last five years, the amount the major medical malpractice insurers have collected in premiums has more than doubled, while their claims payouts have remained essentially flat. The increase in the premiums collected by these companies was 14 times as great as the increase in their claims payments on a gross basis and 21 times as great as the increase in those payments on a net basis (after reinsurance).

• **Incurred losses.** Incurred losses are claims that an insurer projects it will pay in future years on policies in effect in that year. When insurers raise their rates to a much greater extent than their actual claims payments would justify, they argue that the rate increase is necessary because they must increase their reserves to account for what they expect will be higher claims payments in the future. However, the report shows that some malpractice insurers substantially increased their premiums while both their claims payments and their projected future claims payments were decreasing.

• **Surplus.** Surplus is the extra cushion an insurance company accumulates over and above the amount it has set aside to pay its estimated future claims. Because of the overall surge in malpractice premiums with no corresponding surge in claims payments during the last five years, the leading malpractice insurers have increased their surplus by more than a third in only three years, and they are now charging more for malpractice insurance than either their actual payments in malpractice cases or their estimated future payments in malpractice cases would justify.

Data available on specific companies

The following companies are examined in the report: Lexington Insurance Co.; GE Medical Protective Co.; The Doctors Company; ISMIE Mutual Insurance Co.; Health Care Indemnity Inc.; MAG Mutual Insurance Co.; Medical Assurance Co.; ProMutual Group; First Professional Insurance Co.; State Volunteer Mutual Insurance Co.; NORCAL Mutual Insurance Co.; ProNational Insurance Co.; Continental Casualty Co.; American Physicians Capital Inc.; and Evanston Insurance Co.

These are some of the specific company findings:

• Health Care Indemnity Inc. (HCI), an affiliate of HCA, increased its premiums by $173 million, or 88%, while its claims payments fell by $74 million, or 32%. As a result, in 2004 it paid out only 43 cents in claims for each premium dollar it collected.

• Lexington Insurance Co,, an affiliate of AIG, reported that its net written premiums increased from $21.1 million in 2000 to 483.0 million in 2004 — an increase of $461.9 million, or 2200% — while its net paid losses increased by only $52.9 million. As a result, in 2004 it paid out only 14 cents in claims for each premium dollar it collected.

• ProNational Insurance Co., an affiliate of ProAssurance Corp., increased its premiums by $87 million, or 79%, while its claims payments fell by $43 million, or 63%. As a result, in 2004, it paid out only 13 cents in claims for each premium dollar it collected.

• Medical Assurance, another ProAssurance affiliate, increased its premiums by $151 million, or 89%, while its claims payments fell by a third. As a result, in 2004, it paid out only 10 cents in claims for each premium dollar it collected.

The full CJ&D report is available on the group's web site at www.centerjd.org. ■

Median awards on an upward trend in cases

Plaintiff awards for medical malpractice cases are on the rise, according to a report from Jury Verdict Research, a company in Palm Beach Gardens, FL, that analyzes verdicts. Plaintiffs received a median malpractice award of $1.2 million in 2003, up from $1 million in 2002.

But there is some good news in the numbers, says **Jennifer Shannon**, managing editor of the company's reports.

"Even though we're showing the median medical malpractice award is a bit higher in 2003, we are still showing that the odds of a plaintiff receiving a favorable verdict are relatively low," she says. "The new study reports that plaintiffs have a 36% chance of receiving a favorable verdict."

Since 1997, the award median for medical malpractice cases has been increasing, except for a small decrease in 2001, and the trend continues through 2003. The median award for medical malpractice, overall from 1997 through 2003, is $753,901. The award median reflects the middle value of awards listed in ascending order, so Shannon says it provides the most accurate gauge of nationwide trends. ■

Technology is but one solution to e-mail security

(Editor's note: This the last in our series of articles on the risks of using e-mail in health care.)

Electronic safeguards for e-mail in health care, like sophisticated encryption systems, are one piece of the security puzzle but cannot be the entire solution, according to the experts. A risk manager must take comprehensive steps to avoid the inherent risks that come from using e-mail for private information and important medical communications.

In addition to encryption and similar protections, a health care provider must do a thorough assessment of how e-mail is actually used in the organization, says **Mark Rasch**, senior vice president and security counsel for Solutionary, a security consulting company in Omaha, NE. Rasch is a former Department of Justice prosecutor who helped form the cybercrime division, and he now advises health care providers on electronic security.

"You should ask how people are using e-mail, and that's more than just how they say they're using it," Rasch says. "Look at telecommuting, for instance. Are people using e-mail at home and using personal e-mail systems at home, without any safeguards, to transmit protected health information?"

Not necessary to ban some usage

Rasch points out one common myth about e-mail communication in health care: Other than the obvious, like profane or criminal content, he says it is not necessary or productive to forbid discussing certain types of information in e-mail. Even if you try to forbid communicating protected health information by e-mail, people will still do it, he says. And it can be just silly to require to people print out digitally stored documents and walk them down the street to someone else who will scan them into a digital storage system.

"The better alternative is to provide them a way to transmit the document electronically but to do it securely," Rasch says. "That's something you can enforce much more effectively than telling them not to do it at all."

Ultimately, some information must be communicated in some manner, and the alternatives are often no more secure than e-mail, Rasch says. Sometimes they are much less secure.

"The average communication transmitted by snail mail is secured with nothing more than a fifteenth of an ounce of spit on the envelope flap," he says. "There is an illusion of security with regular mail but there's no reason to think that is automatically safer than sending the information by e-mail."

Of course, that depends on exactly how you send that e-mail. The postal service promises a measure of integrity and certain safeguards to protect the mail contents, so e-mail must do the same by encrypting the message.

"As long as you take the proper security steps, you don't have to think of e-mail as any less secure than any other method of communication," he says. "The problem is most people don't add the proper security and they just use the e-mail in its most basic configuration."

Without proper safeguards, it can be very easy to make a big mistake with e-mail, says **Kevin Kalinich**, managing director of technology and professional risks for Aon, a Chicago-based provider of risk management services and insurance. Just ask anyone who has ever mistakenly mailed a love note to a co-worker instead of a spouse, or accidentally copied the boss on the mail venting about his incompetence.

Kalinich cites the example of a company that had a database of Prozac users and wanted to e-mail a reminder about updating their prescription information. A careless mistake caused everyone's e-mail to appear in the address line, so each recipient received the addresses of everyone else on the list.

"Someone just hit the wrong button and the addresses appeared in the cc: line," he says. "It's that easy, and health care providers have a lot to lose when mistake happens. A HIPAA violation is not mitigated when you explain that it was a simple typing error."

A burden added

HIPAA creates an added burden for health care providers that other industries may not face. Patients or others whose privacy is violated may sue, as they can in any industry, but health care risk managers must worry about the added threat from HIPAA. That should be plenty of motivation to study the issue carefully, he says.

In addition to the disclosure of protected health information, Kalinich outlines other e-mail risks:

• **Viruses, worms, and other malicious software that can be transmitted by e-mail.**

Not only can the harmful bugs get into your own system, but you can pass them on to others without proper safeguards — both technological and policies, such as warning employees to never open an unknown attachment or an attachment from an unknown sender.

• **An employee may send inappropriate content through your e-mail system, such as libelous comments.**

"The company can be subject to third-party liability for libel, slander, defamation, and other charges when an employee sends something offensive or something inappropriate from your hospital's e-mail system," he says. "Even if there is no legal ramification, you can suffer tremendous damage to your public reputation if inappropriate or offensive e-mail from your system is reported in the media."

Be careful when e-mailing lawyers

Rasch notes that risk managers must be especially careful when transmitting legally sensitive information by e-mail to an attorney, for instance, or someone else within the health care system. If you are discussing a malpractice case and include privileged information in the e-mail, you must be very careful that the message goes to the right person and is not intercepted along the way.

Encryption can help with that risk, but Rasch notes that the security of such sensitive e-mail can be assured only as far the recipient's inbox.

"While I can be assured that you got the e-mail, you're only one who got it, and you opened it, I have no assurance that you have any security on your own network," he says. "If I give my lawyer a file to review after an adverse outcome, I normally wouldn't worry about the lawyer protecting that paper file I sent over. But with an electronic communication, it can be trickier."

HIPAA puts the burden on the sending party to protect information transmitted electronically so Rasch says you must have written agreements on electronic safeguards with anyone you send protected health information to, and that includes your lawyers, Rasch says.

Hackers are another risk for health care providers. A hacker could get into your billing system and generate bills for fake patients and/or procedures, and then divert the payment to his own account, Rasch says. The safeguards for that kind of intrusion are highly technical and you will have to rely on your IT folks to keep hackers at bay.

Rely on IT

But that doesn't mean you should turn over such concerns to the techies and leave it at that.

"The technology determines what you can do, but the risk manager determines what you *should* do," Rasch says.

Risk managers should make an effort to learn the language of electronic security and at least understand the broad issues as they relate to risk management, Rasch suggests.

"Rely on your IT people for technical support and implementation, but have enough understanding of the relevant issues to know when there is a potential problem," he says. "When

someone in a meeting brings up a great new electronic way to communicate, you need to understand enough so you can speak up and say, 'Wait, there could be some security concerns.'"

Kalinich recommends that risk managers organize a regular meeting, perhaps monthly, with IT, human resources, and a physician representative. At the meeting, the parties should discuss any new developments in electronic communication (such as new ways physicians are exchanging files), whether current policies and procedures are sufficient, any technological innovations or problems, compliance, and any need for staff education.

"The communication among those areas is crucial," he says.

Kalinich says most of the risk from e-mail can be controlled with "social engineering" instead of technological changes. For instance, a good e-mail policy will set forth what is appropriate and inappropriate use of the system, including the proper way to set a password.

What's the most common password that people use for their e-mail access? It's "password."

"Even if it's a good password that people can't guess, about 10% of computer users have their passwords stuck to the monitor on a sticky note," Kalinich says. "That's the kind of thing you have to control with a good policy, and a policy that is enforced." ■

Common errors often made in controlling e-mail risks

Mark Rasch, senior vice president and security counsel for Solutionary, a security consulting company in Omaha, NE, offers risk managers these three common failings regarding e-mail:

- **There is no assessment of the risks.** If you don't know what the risks are in your own organization, based on how your people actually use e-mail, you can't address the risks effectively. Don't assume that the risks are the same for anyone in health care.
- **You assume everyone is following the correct policies and procedures.** Not likely at all. People fail to follow rules all the time, either because they just don't know the rule or they're motivated by other needs. Your policies on e-mail use are no different, so don't think a carefully crafted policy is the end of your worries.
- **Risk managers are often brought in far too late in the process.** It is common in health care for e-mail use to take hold in a particular part of the organization, such as radiologists sending images to each other electronically, long before anyone thinks to consult the risk manager. Create a culture in which everyone is aware that there are significant risk management concerns with all electronic communication and that you should be consulted from the start.

Rasch says you want to avoid someone stopping you in the hall and saying "Oh by the way, we've been doing this by e-mail for six months. That's OK, isn't it?" ■

JCAHO issues alert on fatal misuse of a powerful drug

Patients undergoing chemotherapy to fight leukemia and lymphoma are sometimes being accidentally injected with a powerful cancer-fighting drug in an incorrect way that results in death or permanent paralysis, according to an alert issued by JCAHO.

The drug vincristine has been widely and successfully used to treat cancer for many years, but the Joint Commission reports that the drug is sometimes mistakenly administered in the sac around the spinal cord ("intrathecal") instead of intravenously. The Joint Commission reports that the intrathecal injection of vincristine can be the result of a single error or a series of mistakes in a medication system.

These errors have continued to occur despite repeated warnings and extensive labeling requirements and standards. The Joint Commission issued the alert recently to more than 4,500 accredited hospitals nationwide to create new awareness of the problem and offer practical solutions to protect cancer patients from this type of medication error.

Michael R. Cohen, RPh, MS, ScD, president of the Institute for Safe Medication Practices in Huntingdon Valley, PA, says risk managers must act.

"This tragedy is so preventable, yet there have been many cases reported in the media of patients being injected with vincristine intrathecally," Cohen says. "These cases are especially tragic because the patients experience paralysis

and a slow and extremely painful deterioration, which in nearly all cases results in death."

To reduce the risk of wrong-route errors involving vincristine, the Joint Commission recommends that health care organizations take these steps:

- Dilute the drug in such volume that it prevents intrathecal administration.
- Clearly label all vincristine syringes with this warning: "FATAL IF GIVEN INTRATHECALLY. FOR IV USE ONLY. DO NOT REMOVE COVERING UNTIL MOMENT OF INJECTION."
- Prevent IV and intrathecal medications from being dispensed or administered at the same time, in the same place, ensuring rather that these two distinct procedures are carried out at different times and locations.
- Have at least two caregivers conduct a "time out" before the patient receives vincristine to independently confirm the correct patient, the correct drug, the correct dose, and the correct route for administering the drug. ■

Hospital uses high-tech system to check for errors

Every year, pharmacists at the University of Michigan's C.S. Mott Children's Hospital in Ann Arbor prepare a million doses of medicines for thousands of young and often very ill patients.

And because many of those medicines don't come in sizes or strengths for use in babies, children and teenagers, the pharmacists and technicians must mix many doses themselves. For some drugs, the smallest error in preparation can be a matter of life and death, so the pharmacy team takes special care to double-check every one.

Now they are using a new high tech addition to increase the level of safety to the mixing and dispensing of high-risk intravenous drugs like blood thinners and painkillers. But it's not a standard piece of pharmacy equipment. In fact, it started out in bomb detection.

The new team member is a 2-foot-long blue machine called the ValiMed system, which sits on the countertop in the Mott pharmacy. UM Pharmacy Services director **Jim Stevenson**, PharmD, explains that the machine flashes ultraviolet (UV) light into tiny samples of medicines, instantly checking their identity and concentration just before they're sent to a patient. The system is based on the fact that for most drugs a unique "fingerprint," called a fluorescence signature, can be detected when they are exposed to UV light, he says. Every drug's fingerprint is different.

The UM Health System is the first medical center in the world to use ValiMed for this purpose. The technology was first developed to detect explosives, and is being used at three other hospitals to verify that narcotic drugs aren't being diverted. In addition to watching for pharmacy errors, the system can help monitor for impaired physicians, drug theft, and counterfeit drugs.

Provides another level of safety

Stevenson says the ValiMed system, manufactured by the CDEV Co. in Rockville, MD, eliminates the small amount of potential for human error that remains even with a skilled, trained, and experienced pharmacy team.

"No matter what we humans do to check, double-check, and triple-check our work, there's still that chance for an error to slip through; and with children, especially, there's a lot of drug preparation and the risk to the patient from a medication error can be catastrophic," he says. "In this case, the technology can assure us that we're giving the patient the right drug, in the right concentration, just before it goes to the patient's room. It is the ultimate final check."

The system currently is in use at Mott Hospital, and another ValiMed system soon may be installed at the main University Hospital that treats adults. Stevenson says the machine is just the latest addition to an ongoing patient safety effort by the Mott pharmacy team.

In fact, the pharmacy staff has worked with ValiMed staff in recent months to set the standards that the machine uses to identify drugs. Every time it scans a 1 mL sample of a medication, the machine compares the sample's fluorescent "fingerprint" with a library of standard fingerprints in its memory. UM pharmacists worked with the manufacturers of ValiMed to create that library for high-risk medications, and performed pilot testing of the system before implementing it at Mott.

Can catch potentially harmful mistakes

The current reference library includes 10 commonly used intravenous drugs that need to be mixed specially for children and carry an especially

high risk if they are delivered in the wrong concentration or to the wrong patient. Often, Stevenson says, pharmacists will make a batch of these drugs to dispense to many patients, using bulk medications and IV solution to dilute them so they can be delivered intravenously. Then, for each patient who needs the drug, the pharmacist will fill an IV bag or syringe for the nurse to administer. This means that if a mistake is made in creating the batch, many patients can suffer.

With ValiMed in place, the Mott pharmacists have incorporated a new step into their routine: they draw a tiny sample of the finished IV product, place it in a small square test tube that plugs into the top of the ValiMed machine, wait approximately 30 seconds, and read the machine's display. It tells them if the fluorescence fingerprint from the sample matches the fingerprint for the same drug and concentration from the library.

"We know that medication errors are already extremely rare at Mott, and anywhere at UM, but our goal is to not have any at all," Stevenson says. ■

Joint Commission starts random validation surveys

If you enjoyed your triennial survey, here's a chance to do it all over again the next week. JCAHO recently announced that it has begun random announced "validation surveys" (RAVs) to assess how well the new triennial survey process is working.

The RAVs will assess how well the triennial surveys assess an organization's compliance with Joint Commission standards. RAVs are conducted within two weeks following the triennial survey for selected hospitals.

Not everyone will be subjected to an RAV. Randomly selected hospitals will hear from the Joint Commission within seven days of their triennial survey and be asked to participate in a validation survey within the next seven business days. Hospitals can say no, but those participating will not be charged for the RAV and the findings from the validation survey will not have any impact on the results of the triennial survey or accreditation status.

The surveyors will not have information regarding the outcome of the hospital's recently completed triennial survey, but they will have the priority focus process information and the results of the triennial survey prior to the most recent triennial survey. The RAV will take about as long as the triennial survey.

The Joint Commission will not provide the hospital a report from the RAV visit, but the information will be included in an aggregate report after the project ends in 2006. ■

Reader Question

Reviewing trouble spots ensures good compliance

Question: I think we've done a good job of educating our staff about compliance with the Emergency Medical Treatment and Labor Act (EMTALA), but I still worry that someone will slip up. How can I be sure we've done all we can to comply with EMTALA?

Answer: You can't let your guard down with EMTALA, warns **Linda Parish**, JD, a partner in the litigation and health care section of the law firm Jackson Walker LLP in Houston. No matter how good your compliance efforts have been so far, you must periodically reassess your EMTALA education and awareness levels, plus how well your policies and procedures are actually followed in the hospital.

Parish advises risk managers to thoroughly assess EMTALA compliance at least once a year. An annual review will help you stay compliant even with a high turnover rate of staff in the emergency department, she says. A key part of the review should be verifying that all emergency staff have participated in an EMTALA education course recently, and any new staff who have not should be scheduled immediately.

"It's a good idea at this point to sit everyone in the emergency department down for at least a little refresher course, if not a more complete educational effort," she says. "Everyone can use a reminder. Hospitals get into trouble a lot just because people start talking about insurance or financial status before the screening, without even realizing they're doing anything wrong."

The annual checkup also will involve a review of your organization's policies and procedures, but it doesn't stop there. For instance, Parish notes that you should review the medical staff bylaws because a lot of EMTALA compliance activities are based on those rules.

"There's a limit to how much you can do with your own policies and procedures," she says. "Ultimately you have to depend on the physician to do what he or she should do regarding EMTALA, and that's going to depend on the bylaws."

The bylaws should specify a time period in which medical specialists have to report to the emergency department, as well as a backup plan for when the on-call physician can not respond in a timely manner. Make sure that physicians on call are aware of the requirements, including any specific limits during the on-call period such as not being too far away from the hospital or not scheduling elective surgeries.

"It also is important to remind the physicians that they will have to get up and come to the hospital, rather than trying to handle the call by phone," Parish says. "And remind them that they can not discuss the financial status of the patient before examining him. It's easy for doctors to think that the EMTALA obligation has passed once they get a call at home, but that's not necessarily true."

Parish says you should ensure during your annual review that there is a procedure for what staff are to do when an on-call physician does not respond. The procedure should clearly indicate how many times staff should try to reach the physician, and how long they should wait for the physician to show up before taking other action.

"You want to avoid a situation in which staff just keep trying to reach the doctor over and over, or they let the patient wait forever because the doctor said he was coming," Parish says. "There should be a clear procedure in which the staff takes other action, such as calling the backup physician, instead of just waiting."

With your facility's own staff, your EMTALA review should ensure that policies and procedures are up to date, especially since the law has changed significantly in the past few years. Parish suggests taking a close look at who is allowed to do the initial medical screening examination. Though EMTALA allows a nonphysician to conduct the screening, Parish advises having a policy that requires a physician to do the exam.

"You're just asking for trouble if you have anybody other than an MD do that initial examination," she says.

(Editor's note: Do you have a question about EMTALA or any other risk management dilemma? Send your question to Healthcare Risk Management, *and we will find an expert answer for an upcoming issue. Your name and affiliation will not be published. Contact editor Greg Freeman at Free6060@bellsouth.net or* Healthcare Risk Management, *Attn: Lee Landenberger, 3525 Piedmont Road, Building Six, Suite 400, Atlanta, GA 30305.)* ■

COMING IN FUTURE MONTHS

- 100% physician support for CPOE system
- EMTALA's 250-yard rule still unclear
- Helping physicians communicate clearly to reduce errors
- Latest devices to prevent falls

CE objectives

After reading this issue of *Healthcare Risk Management,* the CE participant should be able to:

- **Describe** legal, clinical, financial, and managerial issues pertinent to risk management in health care.
- **Explain** how these issues affect nurses, doctors, legal counsel, management, and patients.
- **Identify** solutions, including programs used by government agencies and other hospitals, for hospital personnel to use in overcoming risk management challenges they encounter in daily practice. ■

CE Questions

Nurses participate in this continuing education program by reading the issue, using the provided references for further research, and studying the questions at the end of the issue. Participants should select what they believe to be the correct answers, then refer to the list of correct answers to test their knowledge. To clarify confusion surrounding any questions answered incorrectly, please consult the source material. After completing this activity each semester, you must complete the evaluation form provided and return it in the reply envelope provided in order to receive a certificate of completion. When your evaluation is received, a certificate will be mailed to you.

9. What is the main allegation in the report, "Falling Claims and Rising Premiums in the Medical Malpractice Insurance Industry?"
A. Medmal insurers are overcharging health providers for premiums.
B. Medmal insurers are undercharging health providers for premiums.
C. Abuse of the court system by trial attorneys is primarily responsible for high premiums.
D. Premium prices can be explained by the rate of inflation.

10. What does R. Stephen Trosty, JD, MHA, CPHRM, recommend risk managers do in response to the CD&J study?
A. Request a thorough explanation of how premiums are priced from your insurance provider and seek a fuller understanding of how the industry works.
B. Ignore the study completely.
C. Demand a refund of premium overcharges from your insurance provider.
D. Seek an insurer that will not charge premiums in the way described by the CD&J report.

11. According to Mark Rasch, which of the following is true regarding e-mail use in health care?
A. It should be restricted to use only by senior executives and physicians.
B. It is not necessary to forbid including protected health information in e-mail.
C. Protected health information should never be sent by e-mail
D. Encryption is of little use in a health care setting.

12. How often does Linda Parish, JD, suggest you thoroughly assess your organization's EMTALA compliance?
A. At least monthly
B. At least twice a year
C. At least annually
D. At least every two years

Answers: 9. A; 10. A; 11. C; 12. C.

Healthcare Risk Management's
Legal Review & Commentary™
A Monthly Supplement

Denial to hospital admittance results in a suicide; $242,500 settlement in Texas

By **Jan J. Gorrie**, Esq.
Buchanan Ingersoll PC
Tampa, FL

News: A man diagnosed with bipolar disorder became extremely depressed. Believing that he required full-time professional care, his family physician arranged for admittance to a psychiatric hospital. The hospital, however, refused to admit the patient because the admissions staff did not think that he met the criteria for institutionalization. The man killed himself the following day. After filing a lawsuit against the hospital and its individual employees involved in the decision to turn away the decedent, the plaintiffs settled with the defendants' insurance carriers for $242,500.

Background: A widower had become extremely depressed over the one-year anniversary of the death of his wife of 41 years. Realizing that the man already had been diagnosed with bipolar disorder, a brain disorder causing unusual shifts in mood, energy, and the ability to function, the man's family physician determined that her patient posed a significant risk for suicide. The doctor decided that the man needed full-time professional care and she monitored him in her office until he could be transferred directly to a psychiatric hospital.

When he arrived at the psychiatric hospital, a nurse and a physician assistant assessed his condition. Subsequently, the doctor in charge of psychiatric admissions determined that the man did not meet the criteria for institutionalization and declined to admit the patient. Fewer than 18 hours later, the man killed himself.

On behalf of their deceased father, the man's son and daughter filed suit against the hospital, the nurse, the physician assistant, the physician assistant's employer, and the doctor in charge of admitting. The plaintiffs alleged that the defendants negligently refused to provide psychiatric care to their father, even though he posed a significant risk of killing himself. The plaintiffs further contended that this conduct directly and proximately caused their father's subsequent death. The defendants denied that they acted negligently, arguing that the decedent failed to meet the criteria for admission to the psychiatric hospital. The defendants recognized that the man had exhibited some suicidal ideation, but they determined that he did not have a plan or the ready means to commit suicide. Furthermore, the defendants contended that the decedent, upon being denied admission to the psychiatric hospital, had agreed to return to his family physician to undergo outpatient therapy. Because the patient willingly entered this contract for safety, the man's subsequent suicide was beyond the defendants' control.

To prepare for trial, each party retained three expert witnesses in the fields of psychiatry, psychiatric nursing, and hospital administration and procedures. Nevertheless, all parties, fearing the unpredictability of a jury, entered into settlement agreements before the trial began. The insurance

carrier of the doctor, the physician assistant, and the physician assistant's employer agreed to pay the plaintiffs $85,000; the hospital settled for $157,500.

What this means to you: The leading cause of a sentinel event, as reported by the JCAHO, is patient suicide. Root-cause analysis shows the leading contributory cause is environmental safety and security, which was a factor in more than 85% of the cases. But it is followed closely by patient assessment, which was present in four out of five cases.

"Clearly, this is a tragic case. However, predicting suicide is not a science. There are only very rudimentary assessment tools available to even the most skilled health care providers. And, if the judgment regarding psychiatric treatment turns out to be wrong, even the most exemplary assessment will not necessarily carry the day for the defense," notes **Ellen L. Barton**, JD, CPCU, a risk management consultant in Phoenix, MD.

There are several important facts about this case that should be noted.

"First, the concern regarding the patient's suicidal tendencies was made by a medical professional — not a layperson. Second, the hospital involved was not a community hospital that had a psychiatric service but rather a psychiatric hospital where one would presume a higher level of expertise in the evaluation and assessment of a potential psychiatric patient. Third, the patient had a serious, previously diagnosed underlying mental illness of which the admissions staff was aware. Thus, one would assume that these three factors would have argued strongly for the admission of this patient — the fact that a medical professional had concerns, the fact that the facility was a psychiatric facility, and the fact that the patient had a significant brain disorder. Unfortunately, the interplay of these factors seems to have had the opposite effect. The heightened scrutiny that one would expect based on the three factors outlined above led not one, but three mental health professionals to assess the patient as not meeting the criteria for admission," says Barton.

"From the brief facts provided, it appears that the psychiatric hospital followed an established protocol whereby the patient was assessed initially by a nurse and a physician assistant with a final assessment and determination by the physician in charge of admissions and a professional judgment was made that although there was clearly suicidal ideation, the patient lacked a plan and the ready means to follow through. Perhaps, however, given the fact that the patient's personal physician had made the referral, the psychiatrist should have had a follow-up call with her to gain additional perspective on this patient. In addition, while it might be suggested that given the underlying mental illness, this patient's family should have been notified, that course of action would be fraught with HIPAA [Health Insurance Portability and Accountabilty Act] hurdles," she adds.

"The hospital is left with reviewing the clinical standards used to assess patients to see if they meet the criteria for admission. In this context, it would seem most important to take into account the patient's personal history — particularly the death of his wife after 41 years of marriage — as well as his medical history, which in this case was a serious underlying mental illness. It also would seem to be prudent that where another health care provider is involved, as the patient's personal physician was in this case, that discussions with that health care provider be considered mandatory prior to admission determinations," notes Barton.

"The personal situation of the patient also plays heavily in the determination of whether to settle or try a case. The fact that the patient was a recent widower and the fact that he had an underlying mental illness would make him

extremely sympathetic to any jury. The very fact that this individual harmed himself may be viewed as proof of negligence;" she says, "sadly, such cases happen and seem to be among the most difficult to defend.

"The JCAHO sentinel event policy provides that suicide 'of any individual receiving care, treatment or services in a staffed around-the-clock care setting or within 72 hours of discharge' is a reportable sentinel event. So, presuming that the psychiatric hospital is JCAHO-accredited, this case could go either way. However, the patient was screened by facility staff and even though he was not admitted, since his suicide fell within the prescribed 72-hour period, whether reported or not, the facility would do well to perform a root-cause analysis of the case with particular focus on their screening and admission criteria," notes Barton. ■

Post-surgical drugs get the blame in $500,000 verdict

News: After undergoing brow-lift plastic surgery, a young woman blamed her subsequent delirium on the adverse effects of the post-surgery drugs she was prescribed. Three days after surgery, she was treated at an ED for anxiety. Following discharge, she attempted to drown herself and her 6-year-old child. The woman claimed that she should have received appropriate treatment by the plastic surgeon, ED doctor, and the hospital, and also that if more suitable and timely care had been provided, the harm she inflected upon herself and her child would have been avoided. She was awarded $500,000, which was reduced by 40% for her own negligence.

Background: The plaintiff, 24, underwent elective endoscopic brow-lift surgery. The office procedure was performed by a plastic surgeon. Her anesthetic and pre-anesthetic agents included droperidol. After the procedure, the patient received narcotic analgesics that included Norco. She was discharged three hours after the successful procedure was performed.

Immediately following surgery, the patient claims she began to experience agitation, anxiety, and motor restlessness, symptoms that continued after discharge from the surgeon's office. She called the physician's office from home and reported her distress and symptoms to a nurse. She also claimed that the plastic surgeon called her at home the next day, but the medical records contained no notation of the conversation.

The patient claimed that her symptoms worsened and she eventually experienced drug-induced delirium. On the third postoperative day, the plaintiff went to a hospital ED, where she was treated for anxiety and breathing difficulties. During that visit, she failed to tell the treating physician that she had undergone surgery three days prior and that she was on post-surgical medications. She was discharged home and claimed to have reported the ED visit to the plastic surgeon.

After being discharged from the hospital, the patient picked up her 6-year-old child from school and attempted to drive to a beach with the intention of drowning herself and her daughter. On the way to the beach, she became disoriented. When she was unable to find her way to the beach, she stopped the car on an overpass, which she jumped from with her daughter in her arms. They were injured in the fall, but neither was killed. The plaintiff sustained a liver laceration and an elbow fracture. She was charged with attempted second-degree murder.

A psychiatric evaluation concluded that she suffered from a substance-induced delirium at the time of the jump. Based on the diagnosis, she was able to plead not guilty to the crime by reason of mental disease. She brought suit against the plastic surgeon, emergency physician, and the hospital, claiming that they were negligent in failing to properly evaluate and treat her. She claimed that in each of the two times she contacted the plastic surgeon's office, she should have been referred for hospitalization. The plaintiff conceded at trial that she did not tell the emergency physician or anyone at the hospital about her plastic surgery or the post-surgical drugs she was taking, and the hospital and the emergency physician were subsequently dismissed from the case. The plastic surgeon claimed that he only spoke with the plaintiff once after surgery and that drugs used during the surgery and prescribed afterwards could not have caused the patient's delirium. The plastic surgeon contended that the suicidal behavior was not consistent with delirium because she exhibited decision-making ability and the ability to operate a motor vehicle.

A $500,000 verdict was returned against the plastic surgeon. However, this amount was reduced by the finding that the plaintiff was 40% at fault for not disclosing the fact that she had undergone plastic surgery and was on medication

during her visit to the ED.

What this means to you: "One always has to remember that you take the 'patient as you find him or her,' which is true whether the presenting diagnosis is physical or mental. Thus, it would behoove the plastic surgeon to institute a formal evaluation program prior to accepting anyone for elective surgery. Part of the evaluation should be a thorough review of the medical history of prospective patients, particularly past reaction to any drugs that may be used. Another part of the evaluation should be a psychological assessment of the prospective patient to assure a thorough understanding of the procedure, the desire for the procedure, and an assessment of the ability to comply with discharge instructions," notes **Ellen L. Barton**, JD, CPCU, a risk management consultant in Phoenix, MD.

"In addition to a pre-surgical evaluation program, the plastic surgeon should also adopt a more formal follow-up program, especially given that so many plastic surgery procedures are done on an outpatient or same-day surgery basis where patients cannot be monitored for any significant length of time. Thus, in addition, to providing a written set of discharge instructions, follow-up telephone calls should be made to patients on post-op day one and three or, whatever combination is deemed appropriate given the procedure, patient, and other pertinent factors," adds Barton.

"Had post-op calls been made, or as in this instance when the patient called the plastic surgeon's office after her surgery and spoke with a nurse, complete documentation of the calls and any necessary follow-up steps should be instituted. It's not enough to make the calls if there's no follow-through on the follow-up," says Barton. "In this case, if the nurse had any concerns about the patient, the call should have been referred to the surgeon. And it appears from the conflicting stories that he was not made aware of any issues or concerns identified by staff.

"When the patient does not provide relevant information to health care providers, which in this case were the emergency room nurse and physician, it is difficult to hold those health care providers accountable for consequences over which they had no control. While physicians and nurses can try to elicit patients' symptoms, practitioners are not mind readers. The only thing that the emergency department personnel could have done differently was to question her more thoroughly regarding recent activities, surgeries, and medications. But even then there is no guarantee that the patient would have said anything different. Thus, documenting the information exchange is the only risk management tool available to health care providers in the ED in this situation," notes Barton.

"The issue of sentinel events as applied to this case is interesting. First, the surgery was performed in a physician's office; thus, it is assumed that the setting was not JCAHO accredited; therefore, the JCAHO sentinel event policy would not apply. Second, with regard to the hospital emergency room and assuming that the facility is JCAHO-accredited, this situation seems to fall within the cracks. As noted earlier, the JCAHO sentinel events policy provides that suicide 'of any individual receiving care, treatment or services in a staffed around-the-clock care setting or within 72 hours of discharge' is considered a 'reportable' event. The patient, however, did not commit suicide; she merely lacerated her liver and fractured her elbow. Therefore, it would appear reasonable to conclude that this was not a 'reportable' event since the injuries did not occur on hospital premises," Barton explains.

Reference

- Suffolk County (NY) Supreme Court, Index No. 766/01. ■

HIPAA Regulatory Alert

Supplement to Healthcare Risk Management and Hospital Access Management

Ruling on criminal prosecution under HIPAA raises furor

Critics say legal opinion will allow those who abuse privacy information to escape prosecution

A Department of Justice legal opinion, issued at the request of the Department of Health and Human Services (HHS), stated that only covered entities and those people rendered accountable by general principles of corporate criminal liability may be prosecuted under criminal enforcement provisions of the HIPAA Administrative Simplification section.

The opinion has been attacked by privacy advocates, who say it will allow people who misuse privacy information to escape prosecution.

HHS had asked whether the only people who may be directly liable are those to whom the substantive requirements of the subsection apply — health plans, health care clearinghouses, certain health care providers, and Medicare prescription drug card sponsors — or whether the law may also render directly liable other people, particularly those who obtain protected health information in a manner that causes the person to whom the substantive requirements of the subtitle apply to release the information in violation of the law.

Who is liable?

In the opinion he wrote for HHS, **Steven Bradbury**, principal deputy assistant attorney general, said the department had concluded that health plans, health care clearinghouses, those health care providers specified in the law, and Medicare prescription drug sponsors may be prosecuted for violations of Section 1320d-6.

In addition, he said, depending on the facts of a given case, certain directors, officers, and employees of these entities may be liable directly under Section 1320d-6 in accordance with the general principles of corporate criminal liability, as those principles are developed in the course of a particular prosecution.

"Other persons may not be liable under this provision," Bradbury wrote. "The liability of persons for conduct that may not be prosecuted directly under Section 1320d-6 will be determined by principles of aiding and abetting liability and of conspiracy liability."

While Bradbury did not go into detail on the principles of corporate criminal liability, he noted that, in general, the conduct of an entity's agents may be imputed to the entity when the agents act within the scope of their employment, and the criminal intent of agents may be imputed to the entity when the agents act on its behalf.

"In addition, we recognize that, at least in limited circumstances, the criminal liability of the entity has been attributed to individuals in managerial roles, including, at times, to individuals with no direct involvement in the offense," he wrote.

"Consistent with these general principles, it may be that such individuals in particular cases may be prosecuted directly under Section 1320d-6," Bradbury continued.

Other conduct that may not be prosecuted under Section 1320d-6 directly may be prosecuted according to principles either of aiding and abetting liability or of criminal liability, he wrote.

Attorneys surprised at HHS direction change

The ruling limiting prosecution came as a surprise and a disappointment to many privacy advocates and attorneys.

Peter Swires, a law professor at The Ohio State University in Columbus who was chief counselor for privacy in the Office of Management and Budget in the Clinton administration, tells *HIPAA Regulatory Alert* that this opinion is helping the

Bush administration turn the medical privacy law into little more than a voluntary standard.

"Unless the administration pulls back from its current position, it will be up to Congress to protect privacy and say that obviously criminal behavior should be punished by criminal law," he says.

Swires says he has heard that the department pushed hard for this ruling, much to the consternation of some Justice Department attorneys who don't agree with it and are looking for other ways to prosecute those who misuse privacy data.

According to Swires, the HHS Office of Civil Rights (OCR), which has been given the job of civil enforcement of HIPAA, has done little to address the more than 13,000 HIPAA privacy complaints it has received in the past two years. OCR has yet to bring a single enforcement action, he says, and that lack of enforcement sends a signal to covered entities "that HHS will not act even against flagrant violations of the privacy rule."

With no civil enforcement actions, the only success has been on the criminal front, Swires says, and that involves just one case — a hospital lab phlebotomist who accessed the records of a patient with a terminal cancer condition, got credit cards in the patient's name, and ran up more than $9,000 in fraudulent charges, mostly for video games.

Under a plea agreement, the lab technician was sentenced to 16 months in jail. At the time the technician was prosecuted, the Department of Justice said the case "should serve as a reminder that misuse of patient information may result in criminal prosecution," but Swires says it now is possible he will have to be released because under the new opinion he could not be criminally prosecuted because he is not a covered entity (although it is possible he could be prosecuted for identity theft).

Swires says these are among the reasons why the opinion is bad law:

1. The statute applies to "a person who knowingly and in violation of this part. . . ." While the opinion defines "person" only as a covered entity, Swires says the natural reading would include hospital employees who abuse medical records.
2. The criminal statute includes jail time, and real people are sent to jail, not hospitals and health insurance companies.
3. The attorneys who wrote the opinion overlook the fact that Congress made it a crime for any person to illegally obtain health information and insist that Congress was not concerned about criminal activities by outsiders who steal medical records or by insiders who sell medical records or use them for their own advantage, but rather Congress only wanted to target covered entities.

Robert Gellman, a privacy consultant, tells *HIPAA Regulatory Alert* that problems with misuse of medical records are much more likely to involve lower-level staff people in health care organizations who have access to the records than the physicians who are covered.

"Whether there are other criminal penalties that can be applied to those who have been let off the hook by the opinion remains to be seen," he continues.

Gellman says one reason the department might have pushed for this opinion is that it will mean less work to be done and the agency already has shown in civil enforcement that it doesn't want to do much work.

"It appears that OCR has little interest in HIPAA," he adds.

Greatest impact may be in the future

In the short term, the opinion may not have much of an impact because there already is very little enforcement, Gellman points out.

In the longer term, it may affect President Bush's initiative for more electronic health records and a national health information technology effort, he says.

"HIPAA came about initially because Congress wanted more electronic health transactions," recalls Gellman. "But if more people are able to retrieve more medical information, how can you justify the technology and build public support without a policy to protect privacy?"

Emily Stewart, Health Privacy Project policy analyst, tells *HIPAA Regulatory Alert* the opinion came as a surprise and is seen as a "real blow to consumers in terms of the kinds of recourse they have when their privacy is invaded. It severely weakens the force of a law that is already weak in enforcement." She says her group has a consumer coalition on health privacy and has been talking to the other members about possible steps to strengthen privacy protections.

"We find it very ironic that the Bush administration continues to push for a national health information network without providing good safeguards to protect privacy of health information," Stewart says.

HHS also had asked for an explanation of the element in the criminal enforcement section that talks about enforcement against those who knowingly use or cause to be used a unique health identifier, obtain individually identifiable health information relating to an individual, or disclose individually identifiable health information to another person.

The question from HHS was whether the provision requires only proof of knowledge of the facts that constitute the offense or whether it also requires proof of knowledge that the conduct was contrary to the statute or regulations. The Department of Justice said it had determined that the reference was only to knowledge of the facts constituting an offense.

"A plain reading of the text indicates that a person need not know that commission of an act described in [the subsections] violates the law in order to satisfy the 'knowingly' element of the offense," Mr. Bradbury wrote. "Section 1320d-6 makes the requirements that the act be done 'knowingly' and that it be done 'in violation of this part' two distinct requirements. . . . Accordingly, to incur criminal liability, a defendant need have knowledge only of those facts that constitute the offense." ■

Hospitals don't want fined entities identified

The American Hospital Association (AHA) says it is "troubled" by a Department of Health and Human Services (HHS) plan to publicize the identity of those covered entities given civil monetary penalties under enforcement of HIPAA's administrative simplification section.

The association also says it is especially concerned over the department's expectation that consumers will use the information to help choose a health care provider.

In written comments to HHS, **Melinda Reid Hatton**, AHA vice president, said hospitals had asked that HHS make available to covered entities information about violations, proposed solutions, and good practices in a form that did not identify violators.

"Making information available in an unidentified format would allow covered entities to understand how the Office of Civil Rights and the Centers for Medicare & Medicaid Services interpret and apply the HIPAA regulations in specific cases and would encourage remediation of problems and violations discovered through the enforcement process," she said.

"The information would enable covered entities to gain a better sense of the types of compliance problems that are occurring and the misunderstandings that exist regarding application of the HIPAA regulations," Hatton explained.

But the notion that information about violations of HIPAA technical requirements is useful to consumers is flawed, she noted.

"Consumers should not make their health care decisions based on HIPAA's technicalities. These are irrelevant to the quality of care patients receive from a provider. As the number of complaints filed with the Office of Civil Rights for incidents that are not HIPAA violations suggests, many consumers do not understand these complicated rules," Hatton added.

Moreover, she said, although health care consumers who are informed that a hospital violated the HIPAA medical privacy rule are likely to believe the hospital does not adequately protect patient privacy, most violations of the medical privacy rule are not the result of an impermissible use or disclosure of patient information and are likely to be only technical in nature.

AHA said it appreciates that compliance with technical requirements of the administrative simplification provisions, including the technical requirements of the HIPAA medical privacy rule, is important and that accrediting entities need to know of these facts.

However, it said, the potential for seriously misleading the public about the meaning of the medical privacy rule violations where no impermissible use or disclosure occurred is an unwarranted and irresponsible policy.

Methodologies not easy to understand

Hatton also pointed out that the methodologies used to establish violations and penalties, such as statistical sampling and the number of days a requirement was not met, are not easy to understand.

She cited an example of a potential publicized violation of a hospital that had 1,100 violations of the medical privacy rule in a 90-day period, when the violations would refer to nothing more than that the hospital was unable to document that its Notice of Privacy Practices was acknowledged by people admitted to the emergency department or

that the department had determined that processes used to collect data for the accounting of disclosures with respect to 1,100 patients do not have all the details needed to comply with its guidance.

"As a result," she said, "a statement that Hospital A paid several thousand dollars in fines due to 1,100 violations of the privacy rule arguably is misleading and could panic individuals into distrusting their provider."

In other comments, Hatton:

- endorsed the department's continued emphasis on voluntary compliance;
- urged the Office of Civil Rights and the Centers for Medicare & Medicaid Services to fulfill the enforcement rule's promise to "continue to work on educational and technical assistance materials, including additional guidance on compliance and enforcement and targeted technical assistance materials focused on particular segments of the health care industry";
- called on the government to provide more information to covered entities on the methodologies for establishing any violation and the amount of a penalty;
- expressed concern that the proposed enforcement rule significantly restricts and limits a covered entity's ability to present a defense and appeal an adverse ruling, including imposition of a civil monetary penalty.

[Download the comments from the HIPAA section of www.aha.org. Contact Melinda Hatton at (202) 638-1100.] ■

Transaction standard is far from projected uniformity

The HIPAA transaction standards have not resulted in the uniformity and efficiency envisioned when HIPAA was adopted.

That's the opinion of the HIPAA Implementation Working Group, which were presented in testimony to the National Committee on Vital and Health Statistics.

The group, which represents health care providers, vendors, and clearinghouses, said that for providers, clearinghouses, and many others, standards implementation has yet to result in any clear return on investment.

"The savings predicted by the Department of Health and Human Services of $29.9 billion in administrative expenses over a 10-year period beginning in 2002 are far from view," they said.

"To date, the costs of complying with the Transactions and Code Sets Standards have been significant, and there are no data showing that providers have experienced any return on their investment," the group noted.

The Working Group said significant progress has been made in implementing a standardized electronic claim form through use of the 837 claim transaction.

As 837 use becomes routine, according to the testimony, the industry has begun to discuss implementation of standards for other transactions. Collaboration is increasing among many sectors of the industry to ensure standards have the utility and promote the uniformity envisioned by the law, the group said. In addition, providers and vendors are becoming more active in the standard setting process.

The Implementation Working Group said the benefits of adopting any transaction standard relate primarily to ways in which standardization improves a participant's ability to receive useful detailed information in a timely, uniform, and cost-efficient manner.

"The 837 claim transaction, which has been the primary focus for the HIPAA transition, is bringing limited, if any, benefit to the provider community in part because significant payer-specific customization is still required," according to the group's testimony. "As the focus of implementation shifts to transactions through which health care providers can obtain useful information, the opportunity for a positive business impact from standardization grows. For example, providers expect to see financial benefit from timely and useful patient eligibility, remittance advice, and claim status information."

The group said the degree to which standards implementation has a positive or negative business impact also depends heavily on whether the standards reflect the needs of those who use them. But the current standards do not address the business needs of the provider and vendor communities, due in part to the historically significant representation of providers and vendors in the standard-setting process and in part due to the limited understanding of how the standards would be used in practice.

"We should learn from these experiences and use them to strengthen the standard setting process," the Working Group declared. ■