Healthcare Risk Management®

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

THOMSON
AMERICAN HEALTH CONSULTANTS

IN THIS ISSUE

Financial Disclosure:
Author Greg Freeman, Editorial Group Head Glen Harris, Senior Managing Editor Joy Dickinson, 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.

DECEMBER 2005
VOL. 27, NO. 12 • (pages 133-144)

Want to detect dangerous staff? Use background checks, monitoring

Check any suspicious pattern of deaths, look for common staffer

The story hits the news every once in a while, but it always seems like such an extreme case: A hospital staffer confesses to killing multiple patients over time, usually with fatal injections and often under the pretense of a "mercy killing."

But is there anything a risk manager can do to prevent such a tragedy, or is this such an extreme scenario that it's not worth the effort? Risk managers who have been through this problem say it most certainly is worth your time and effort to screen out these potential killers and spot their crimes as soon as possible.

"If you think you're immune from this kind of problem, you're kidding yourself," says **Peggy Nakamura**, RN, MBA, JD, DFASHRM, CPHRM, assistant vice president, chief risk officer, and associate counsel at Adventist Health in Roseville, CA. She also is a past president of the American Society for Healthcare Risk Management (ASHRM) in Chicago.

Nakamura experienced such a situation in her own organization and she says it opened her eyes to how much risk managers must be proactive in preventing serial killers from harming their patients. In 1998, Efren Saldivar,

EXECUTIVE SUMMARY

Risk managers must act proactively to prevent criminals from being hired into the organization and given the opportunity to harm patients. The potential harm from one "mercy killer" justifies the extra precautions.

- Background checks are a must, even though most employers will not give much information.
- You should have a policy that requires investigation after any pattern of deaths on a unit.
- Temporary staff pose a special risk in this area.

a 28-year-old respiratory therapist at Glendale Adventist Medical Center in Los Angeles, confessed to killing 40-50 patients over the previous decade, mostly with the drugs Pavulon and succinylcholine chloride. He was fired and now is serving life in prison.

Dozens of killings possible

Nakamura presented her advice recently at the recent annual ASHRM meeting, along with **Kenneth N. Rashbaum**, JD, an attorney with Sedgwick Detert in New York City. He was involved with investigating the case of Charles Cullen, a nurse who pleaded guilty in 2004 to the murders of 13 patients at Somerset (NJ) Medical Center. In return for a plea agreement that would spare him the death penalty, Cullen agreed to cooperate with prosecutors investigating patient deaths in five additional New Jersey counties where he had worked as a nurse.

He eventually confessed to using various injections to commit murders at five additional hospitals before going to work at Somerset, Rashbaum reports. Cullen has confessed to about 30 murders at the different hospitals, with the exact number depending on which law enforcement agency is counting. When the Cullen story broke, it revealed the problem that risk managers can face when trying to screen out dangerous employees. Most health care employers will not provide anything more than the bare minimum of information about a past employee — what Rashbaum calls the "name, rank, and serial number" response.

In defending itself against claims that the hospital's negligence allowed Cullen to kill with impunity, Somerset Medical Center pointed out that Cullen had worked at nine other health care facilities over 16 years and had a long history of questionable behavior. But none of those previous employers alerted other health care providers when asked for a reference.

"The hospital said they could have been sued for saying anything negative about the former employee, and they were right," Rashbaum says. "The name, rank, and serial number response is policy at most hospitals because they want to avoid a negligent misrepresentation lawsuit."

The health care industry and state legislatures need to provide protection against such lawsuits and encourage employers to provide full information about past employees, especially any clinician who has displayed dangerous behavior, Rashbaum and Nakamura say. **(See p. 136 for more on providing useful referrals to other health care employers.)** But until that happens, the onus is on risk managers to protect the organization from these killers.

Background checks are first defense

Rashbaum emphasizes that stopping these killers requires a multidisciplinary team. The risk manager may have to take the lead, but human resources and legal counsel must be involved. **(See p. 136 for more on working with those departments.)**

Nakamura says the first hurdle is the naturally benevolent mindset found in most health care

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), $495. 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.

professionals. Health care providers tend to be trusting, she says, but some degree of objective skepticism is necessary. "In our incident, it was impossible to believe, but the facts were presented to us," she says. "We are trusting individuals, and it is hard for us to believe there are criminal minds in health care."

To counter that tendency, Nakamura says you must be skeptical when viewing any reports of suspicious behavior in an employee, especially any that suggest a pattern. Never assume that the incident was just a mistake or misunderstanding, or that the person simply wasn't trained well enough.

The best way to prevent a killer from preying on your patients is to keep him or her out of the facility altogether, say Nakamura and Rashbaum. They advise conducting thorough background checks on all employees, looking for any hint that the person has been involved in criminal behavior before or might have been dismissed from other health care facilities. They offer this advice on background checks:

- Know your own state requirements for background checks and those of adjoining states if you draw employees from over state lines.
- Always verify the applicant's identity, and consider using fingerprinting as the most accurate means of verification. "It's amazing how many applicants have falsified their identity," Nakamura says. "Start with simply verifying that they are who they say they are."
- If the applicant was discharged from the military, ask for a copy of Form DD-214. In addition to verifying the discharge status, the DD-214 may include interesting information about performance, disciplinary action, and psychiatric testing.
- Request a copy of the applicant's last performance review from the previous employer.

"Be suspicious if they don't have it or even the previous one," Nakamura says. "I've always found that people keep copies of their performance reviews, especially the good ones. Watch how they respond to this request."

Rashbaum and Nakamura point out that you must be careful when conducting background checks. If you use conviction records, for instance, your organization should have a specific policy that outlines how you will react to the nature and gravity of the offense, plus the time since the offense. Will you rule out someone who was convicted of a nonviolent misdemeanor 20 years ago?

If you consider arrests in addition to actual convictions, the bar has to be set higher. Nakamura says the conduct leading to the arrest should be related to employment, and you should look to your own state law for further restrictions. If you use an outside agency to conduct background checks, review the contract carefully to see exactly what information the agency will pursue. In particular, you should ask if the agency will be searching in other states, because killers in health care often move from one state to another in an effort to hide their history.

Nakamura also advises risk managers to implement revised data collection procedures in an effort to thwart (or at least detect) any criminals who slip through your screening process. She offers these tips:

- Conduct routine toxicology screens immediately post-cardiac arrest for all patients, without waiting until there is reason to suspect foul play.
- Obtain monthly code and death statistics by unit, shift, and total hospital. Compare units to each other and themselves.
- Require strict pharmacy and unit accounting of all doses of medication. After the incident at Nakamura's facility, the hospital had to change pharmacy practices to ensure that Pavulon was monitored closely.
- Incorporate data from those policies into any root-cause analysis after a suspicious or unexpected death.

SOURCES

For more information on screening for employees with criminal intent, contact:

- **Peggy Nakamura**, Assistant Vice President, Adventist Health System, 111 N. Orlando Ave., Winter Park, FL 32789. Telephone: (407) 647-4400.
- **Kenneth N. Rashbaum**, Sedgwick, Detert, Moran & Arnold, 125 Broad St., 39th Floor, New York, NY 10004-2400. Telephone: (212) 422-0925. E-mail: kenneth.rashbaum@sdma.com.

Keep close eye on temporary staff

Temporary staff pose a special risk, Nakamura says, because they are unknown to others on the unit, and serial killers often move quickly from one facility to another. Risk managers should require enhanced monitoring of temporary staff and in particular, they always should be closely supervised by management and should work alongside regular staff, Nakamura says.

"Avoid having all temporary staff on one unit," she says. "That is really dangerous, especially on a critical care unit."

Managers should closely review temporary staff members' performance and require adherence to all organizational policies. It is never acceptable to overlook poor performance or shortcuts just because the staffer is temporary. Nakamura also advises assigning a senior staff member to "buddy" with the temporary staffer and report to department management.

"Anybody who is new should be watched closely, and temporary staff always represent a risk," Nakamura says. "They may think that they will be long gone by the time anyone suspects anything." ■

Stop killers — work closely with human resources

Creating a better defense against health care workers who would harm your patients means working closely with your human resources department, but prepare yourself for a challenge. The folks in that department have their own important concerns, and you will have to cooperate if you want any meaningful change.

Peggy Nakamura, RN, MBA, JD, DFASHRM, CPHRM, assistant vice president, chief risk officer, and associate counsel at Adventist Health in Roseville, CA, says risk managers have to keep in mind that the most obvious things they want to do in this regard could be a problem for human resources. The best strategy, she says, is to get human resources on board with the idea of preventing this kind of tragedy, and then see how you can work out a solution. Remember that if you have a collective bargaining agreement, that agreement will have to be factored in to the plan.

Here are some of Nakamura's tips:

- Create a policy that requires any employee misconduct be "red flagged" in performance reviews.
- Include in performance reviews any repeated policy or procedure violations, behavioral issues, and complaints from staff.
- Make unaccounted absence from the employee's unit a serious issue that managers are required to document. Serial killers frequently are away from their assigned unit when they do harm to patients or when they are obtaining drugs.
- Require that performance reviews must include a retrospective review of the employee's involvement in incident reports, sentinel events, odd behavior, or medication administration discrepancies.

When you suspect that a staff member or physician may have intentionally harmed a patient, Nakamura says it is imperative that you act quickly. Don't wait for a confession. Seek legal counsel immediately and contact local enforcement as soon as possible.

"Your local law enforcement authorities become very edgy if you don't contact them right away," Nakamura says. "It is absolutely critical to get off on the right foot with local law enforcement. They can be a great ally if you don't send the signal that you're covering up or focused on avoiding liability." ■

Referral of ex-employee can raise legal risks

When a past employee left your organization under questionable circumstances, or with a history of suspicious behavior, it is important to be honest with the next employer who asks for a referral. Experts say an honest referral is the best way to stop a health care worker who moves from one employer to another and eventually harms a patient intentionally. But how can you tell the truth without inviting a lawsuit?

You can if you're careful about how you respond, says **Kenneth N. Rashbaum**, JD, an attorney with Sedgwick Detert in New York City. The fear of reprisal currently limits the disclosure of essential information and frustrates the employer who is left holding the bag when the criminal behavior is finally discovered. The reluctance to say anything negative about former employees is not unjustified, Rashbaum says, but there are ways to change this pattern.

An employee who received a bad referral from your organization can sue for defamation, invasion of privacy, or civil rights claims he alleges if the bad referral was for filing a discrimination claim or a whistle-blower claim. Even a seemingly good reference can result in a lawsuit — a "negligent references" claim — if the employee says you only gave half of the story and left out information that would have made him or her look better to the new employer.

So what's a risk manager to do? Rashbaum says risk managers may have to take the lead in encouraging more honest referrals, and expect your counterparts in human resources and legal to resist.

"This is what we do. We know there's a risk from not telling the truth to other employers, and we need to find a way to change that," he says. "But human resources and legal counsel have their own concerns that are just as valid, so you have to work with them."

Rashbaum says risk managers should work with the other departments on these tasks:

- Check with legal or outside counsel for the privilege statutes in your state.
- When possible, obtain consent for the reference.
- Give the reference letter directly to the employee.
- Train the specific people authorized to respond to reference requests. Any request for a reference must go to one person or one team of people who know what to say and not say.

It is important to check your own state's laws requiring references to see what is protected and what limitations might apply. For instance, North Carolina provides immunity from civil liability unless the information disclosed was false *and* the employer knew or should have known it was false.

In New Mexico, however, state law says employers may face liability for "incomplete referrals" if more than just the name and dates of employment are given.

"So in New Mexico, you have to either provide nothing but name and dates, or you have to provide a full and accurate picture," Rashbaum explains. "An incomplete report can be only half the story and be construed as negative." ■

Risk managers, doctors disagree on 'full disclosure'

Risk managers and physicians have both joined the movement toward full disclosure with gusto, but a recent survey suggests that it is easier to talk about your dedication to informing the patient than it is to actually do it. When it comes to the specifics of exactly what to tell the patient, risk mangers and physicians often disagree and — surprisingly — the physicians are often more in favor of telling the patient the whole story than the risk managers are.

EXECUTIVE SUMMARY

A recent survey reveals that risk managers and physicians may both voice support for full disclosure after an adverse event, but they disagree on what to actually tell the patient. Risk managers also are not unified in what they recommend to physicians.

- Physicians are more in favor of disclosing near misses.
- Risk managers are less certain that disclosure will discourage a lawsuit.
- Physicians are more in favor of using the word "error."

The intriguing results were the result of a survey of 1,798 members of the American Society for Healthcare Risk Management (ASHRM) and 1,233 physicians. The survey results were presented at the recent annual ASHRM meeting by **Thomas H. Gallagher**, MD, assistant professor of medicine at the University of Washington School of Medicine in Seattle, along with **Kerry M. Bommarito**, MPH, and **Alison G. Ebers**, researchers at Washington University School of Medicine in St. Louis.

Gallagher says the results may come as a surprise to risk managers who have jumped on the "full disclosure" bandwagon and think that simply endorsing the concept will bring change to their operations. "We all agree to a great extent on the principles of disclosure, but there is a gap between the principles and what we actually do," he says.

Both groups harbor misgivings

Gallagher notes that it has taken years for risk managers and physicians to accept the idea of full disclosure instead of keeping patients in the dark about what happened to them, but he says the survey results suggest there still is much work to be done if the principles of full disclosure are to be put into practice on an everyday basis. Clearly, he says, physicians and risk managers still harbor some misgivings about telling patients the facts — all the facts, without waiting for the patient to ask — and in some scenarios, the risk managers are more wary than the physicians.

That wariness is counter to the notion, common in many discussions of full disclosure, that risk managers embrace the new approach to full disclosure but are stymied by physicians who fear they will encourage a lawsuit or damage their own

SOURCES

For more information on disclosing errors, contact:

- **Kerry M. Bommarito**, Research Patient Coordinator, Department of Internal Medicine, Box 8051, Washington University School of Medicine, 660 S. Euclid Ave., St. Louis, MO 63110. Telephone: (314) 362-5000. E-mail: kbommarito@wustl.edu.
- **Thomas H. Gallagher**, Assistant Professor, Department of Medicine, Box 356178, University of Washington School of Medicine, Seattle, WA 98195. Telephone: (206) 543-4802. E-mail: thomasg@ u.washington.edu.

reputations. "One explanation is that the health care professional in risk management knows disclosure is the right thing to do but lacks the moral courage to pull it off," Gallagher says. "I tend to favor some more complex explanations."

Plus, Gallagher says, it's not as if physicians are unanimous in their support of full disclosure or consistent in how they practice it. There is a growing concern among some physicians that there now is too much focus on the patient, he says, with no consideration of how disclosure can affect the health care provider.

The survey of ASHRM members and physicians revealed a significant "disclosure gap" in several areas, Gallagher says.

First, the survey results suggest that risk managers are more firmly convinced of the seriousness of medical errors, with 83% agreeing that medical errors are "one of the most serious problems in health care," compared to only 64% of physicians. Risk managers also are far more convinced that medical errors are "usually caused by failures of care delivery systems, not the failure of individuals," with 84% agreeing with that statement, compared to only 54% of physicians.

Physicians do acknowledge that being involved with an error can seriously affect their own lives. Sixty percent of the physicians say a medical error created anxiety about being involved in future errors. Forty-six percent say that being involved with a medical error has affected their confidence as a physician, 43% say it has affected their job satisfaction, 42% say it has interfered with their ability to sleep, and 13% think it has affected their professional reputation.

Despite that angst, physicians aren't all that eager to pursue counseling after a medical error. Twenty percent said they would not be interested at all in counseling after involvement in a serious error, and 52% said they would be somewhat interested. Only 28% said they would be very interested. The biggest barrier to seeking counseling was a concern that it would take time away from the doctor's work, cited by 47% of the respondents. Other common concerns included confidentiality, creating a record of the counseling, effects on malpractice insurance, and thinking that counseling just would not be helpful. **(See article, below, for more survey results, and p. 139 for differences revealed by medical error scenario.)**

Bommarito reports that the survey revealed 71.8% of the risk managers officially have approved disclosure policies at their facilities. Error reporting systems may go unused, however. When asked if their facilities have an error reporting system to improve patient safety, 81% of risk managers but only 37% of physicians said yes.

"Forty-five percent of physicians said they didn't know if their hospital had an error reporting system," she notes. "That's a big problem."

The survey also revealed that risk managers have an inflated idea of how well their error reporting systems work. Fifty-seven percent of risk managers agreed with the statement that their current system for facilitating physician reports about patient safety are adequate, but only 30% of the physicians thought so. When asked about mechanisms for informing physicians about errors in their facilities, 51% of risk managers thought they worked well, but only 18% of physicians agreed. ■

Disclosure gap is apparent with docs

When asked about attitudes toward when and how to disclose, the gap between risk managers and physicians becomes more apparent, with physicians sometimes more enthusiastic, says **Thomas H. Gallagher**, MD, assistant professor at the University of Washington School of Medicine in Seattle. He presented survey results recently at the American Society for Healthcare Risk Management (ASHRM) annual meeting.

Regarding whether near misses should be disclosed to patients, 30% of physicians say yes, but only 19% of risk managers answer affirmatively. Seventy-seven percent of physicians and 74% of risk managers endorse disclosing minor errors to patients. For serious errors, 98% of both groups

support disclosure.

The results suggest that some of the efforts to push full disclosure have been more successful with physicians than with risk managers. For instance, 64.6% of physicians agree or strongly agree that disclosing a serious error will make the patient less likely to file a lawsuit — a fundamental argument in favor of disclosure — while fewer risk managers (58.1%) feel the same way.

On the other hand, it seems that physicians can come up with more excuses for not disclosing the error in a particular situation. When posed with list of potential reasons for not disclosing, physicians consistently were more open to using them. For instance, 30.3% of physicians said they would be less likely to disclose a serious error to the patient if he or she felt the patient did not want to know, compared to only 19% of risk managers. Nearly a quarter of physicians, 23.2%, said they would be less likely to disclose if the patient was unaware that the error happened, compared to only 8.5% of risk managers. Thinking that the physician may get sued would make 23.7% of them less likely to disclose, but it would only discourage 2.5% of risk managers.

The patient's likely inability to understand the information would make 60.6% of physicians and 47.2% of risk managers less likely to disclose. ■

Survey: Doctors respond differently after error

A survey conducted by **Thomas H. Gallagher**, MD, assistant professor at the University of Washington School of Medicine in Seattle, included scenarios that presented medical errors to the physician and risk manager respondents and then asked them how they would disclose the error to patients. The responses revealed startling differences.

In one scenario, a nurse gives a patient 10 times the correct dose of insulin because she misread the physician's sloppily written order. The patient nearly dies but recovers. Both groups were asked if and how they would disclose the mistake. Both favored disclosure, with 11.1% of risk managers and 31.8% of physicians saying they would "probably disclose the error." Another 87.4% of risk managers and 64.8% of physicians said they "definitely would disclose the error."

But they did not agree on how they would disclose. Almost no one opted for the first choice: telling the patient his blood sugar went too low but giving no hint of the insulin overdose. The next option was, "Your blood sugar went too low because you received more insulin than you needed." This not-quite-full disclosure was chosen by 51.4% of risk managers but only 27.6% of physicians.

The third option was, "Your blood sugar went too low because an error happened and you received too much insulin." This wording was chosen by 48.2% of risk managers and 71.4% of physicians.

"So risk managers are evenly split on whether to say 'error' and interestingly, physicians are more in favor of this *full* disclosure of the error," Gallagher says.

In a follow-up question with the same scenario, physicians again were more willing to use the word "error" in their apologies than risk managers. Forty-three percent of physicians were willing to say, "I am so sorry that you were harmed by this error," compared to only 23% of risk managers. The less-specific apology, "I am sorry about what happened," was chosen by 76% of risk managers and 54% of physicians.

Avoiding the word 'error'

Other survey results, however, suggested that surgeons (as opposed to other physicians) will be less willing to use the word "error" when talking to the patient. Surgeons' responses on that issue were more in line with risk managers'.

Gallagher says the survey results, and the discussion by ASHRM attendees at the conference session, suggest that risk managers are sometimes more committed to disclosing "errors" in theory than in practice. When faced with a specific scenario, risk managers often favor stating the bare facts and letting the patient figure out that an error occurred, he says, a position advocated by many of the risk managers attending his presentation.

Gallagher says that reluctance to say the word "error" can backfire if the patient perceives the health professional as evasive or trying to minimize the mistake. "The question becomes what is the minimum information you need to disclose without the patient asking for it," he says. "There's no answer on that yet, but it is clear that dribs and drabs of information, forcing the patient to ask for more and more information, can contribute to the patient's anger." ■

Be voice of reason when sending help

(Editor's note: This month, Healthcare Risk Management *continues its coverage of the risk management lessons from Hurricane Katrina with advice on how to send health care professionals to help without incurring unreasonable risks and how you can comply with federal privacy rules during a disaster. See the November* HRM *for coverage of the importance of planning before a disaster, the likely liability risks and lawsuits that will follow the hurricane experience, and what standards the courts may use as the "best-practice" model for disaster preparedness.)*

Many hospitals outside the area directly affected by Hurricane Katrina had difficulty sending in teams of clinicians because of concerns about liability, says **Lori-Ann Rickard**, JD, a partner with of Rickard & Associates, a law practice in St. Clair Shores, MI, that specializes in health care. Their experience holds lessons for all risk managers, she says.

Special Report: Lessons from Hurricane Katrina

Good Samaritan laws can protect workers if they volunteer, but not if they will be paid by their regular employers, she says. State laws vary greatly and can be highly complex regarding who is covered by immunity clauses, Rickard adds.

"If I were a risk manager at a facility wanting to send physicians, I would want to be apprised of what federal and state laws apply," she says. "If there is a state of emergency in your own state, not just the state where you're sending doctors, that can help protect you a great deal. So does a federal state of emergency. And you need to know what your people are going to be asked to do."

There are plenty of other issues to consider before sending medical crews, she notes. Will your staff have death benefits if they die on the assignment? What are the health risks, and what is your liability for that? Risk managers must be the voice of reason sometimes when people are eager to respond quickly and join a humanitarian relief effort.

"It gets much more difficult than just saying you want to do the right thing and send your staff to help. You have a duty to watch out for them and consider what can happen to the organization," Rickard says. "Some of those people that go are going to die, especially if you're talking about a pandemic, and there will be a need for help 30 days out, 90 days, and 120 days out. You have to remind people that they still have a responsibility to help in their own communities."

She says those issues must be considered as more hospitals are being asked to sign agreements to respond when other communities need medical assistance, often as a requirement for receiving federal emergency equipment and funds. Risk managers should look beyond the paperwork and consider what the agreement actually means.

"You need to keep saying to people, 'Good idea, but what are the risks?'" she says. "You don't want to just do things with good intentions and then you don't exist as an organization because some plaintiff's attorney decided this would be a good thing to sue everyone across the country for."

All of those issues were serious concerns when hundreds of volunteers from Stanford (CA) Medical Center left for the Gulf Coast, says **Pamela L. Popp**, JD, MA, DFASHRM, CPHRM, senior director of claims and litigation at Stanford and immediate past president of the American Society for Healthcare Risk Management in Chicago. Popp says that such situations can be career opportunities for risk managers because they are in a position to provide leadership.

EXECUTIVE SUMMARY

Resist the urge to send relief crews into a disaster zone without first considering the potential risks and liabilities.

- A state of emergency can provide some liability protection.
- Risk managers must be the voice of reason.
- Consider how state laws vary.

SOURCES

For more information, contact:

- **Pamela L. Popp**, Senior Director, Claims and Litigation, Stanford Medical Center, 300 Pasteur Drive, Stanford, CA 94305. E-mail: Ppopp@stanfordmed.org.
- **Lori-Ann Rickard**, Partner, Rickard & Associates, Grosse Pointe Plaza, 22725 Greater Mack Ave., Building B, St. Clair Shores, MI 48080. Telephone: (586) 498-0600.

"People will turn to you in these times and ask, 'What do we do now?'" she says. "And there is good reason for them to look to you for guidance, because there are some very serious risk management issues involved. In a way, this can be very positive, an opportunity for risk managers to showcase their knowledge and experience by becoming an internal resource for their organizations."

Of course, you can do that only if you're ready when the time comes. There may be little notice when a disaster strikes and people in your organization start mobilizing to respond. Plan now for the next disaster, and study the relevant issues calmly and thoroughly, she says. **(For more information, see "When a crisis strikes, turn to your bible of crucial info," *Healthcare Risk Management*, June 2005, p. 67.)**

The alternative, Popp says, is that you may find people coming to you with questions you can't answer during an emergency. If that happens, not only are unable to fulfill your obligation to the organization but you also have squandered an opportunity to shine as a risk manager.

"The limelight can be great, but there are pros and cons to it," she says. "If you have taken advantage of opportunities to learn about these issues ahead of time, you can break out as a real leader when people need that the most." ■

Lack of medical data, HIPAA no hindrance

Special Report: Lessons from Hurricane Katrina

With so many patients evacuated and arriving at other facilities for care after Hurricane Katrina, one of the first questions posed to health care providers was how to comply with the Health Insurance Portability and Accountability Act (HIPAA). Some of those concerns were dispelled when the Department of Health and Human Services issued a special bulletin explaining that HIPAA should not be seen as any impediment to the hurricane response. However, risk managers can learn more about everyday compliance with HIPAA from the Katrina experience, says **Kevin Lyles**, JD, an attorney with the law firm Jones Day in Columbus, OH.

EXECUTIVE SUMMARY

Health Insurance Portability and Accountability Act (HIPAA) restrictions should not stand in the way of providing health care during a disaster. Clarifications issued during the Hurricane Katrina crisis should reassure risk managers.

- The Hurricane Katrina experience yields lessons for everyday HIPAA compliance.
- The government has said it will not aggressively enforce HIPAA during such a crisis.
- Civil lawsuits stemming from privacy breaches still are possible.

The main HIPAA-related problem was that people were calling hospitals to look for displaced relatives and the receiving hospitals didn't know if they could release the information under HIPAA. The HHS bulletin made it clear that they could. **(See p. 142 for more on the HHS bulletin.)**

"HHS really wasn't covering any new ground with that. HIPAA already allowed hospitals to make information available if they deemed it helpful to the patient," Lyles explains. "They were pointing out what HIPAA already said. They did suspend some provisions of HIPAA, such as the requirement of a business associate agreement."

HHS also made clear that the government would pay hospitals for treatment even if they did not follow all provisions of HIPAA. And most importantly for risk managers, HHS stated that it would not take an aggressive enforcement approach in the wake of Hurricane Katrina.

"They basically said that if you act in good faith and have good intentions, we're not going to hold you liable for any HIPAA violations during this emergency," he says. "The agency is the only one that can enforce HIPAA, and they were saying they would not nitpick about HIPAA violations and you should go out and do what you need to do for your community."

Risk managers who didn't experience Hurricane Katrina still can learn lessons about HIPAA compliance, Lyles says. For one thing, he says, the experience shows a need for flexibility in how you write HIPAA policies.

"You need some flexibility in how you will respond to an emergency like this and how you will bend your standard procedures for notification of family members and giving out information," he says. "If you have a policy that assures

patients you will not give out any information without their permission, you might want to build in some leeway with a phrase such as 'except in the case of an emergency or when a public health crisis requires the release of information.'"

That type of language is consistent with HIPAA rules, Lyles notes, but putting it into your own policy is better than having such an ironclad policy that your staff is bound to violate it when they are in a crisis.

"You never want a policy that you don't follow, so it's best to outline those potential exceptions in your own policies," he says.

Even without government enforcement for HIPAA violations, civil lawsuits still could arise, says **Patricia A. Trites**, MPA, CHBC, CPC, CHCC, CHCO, CEO of Healthcare Compliance Resources, a consulting firm in Augusta, MI. Trites says civil actions could arise because of the lack of compliance with the Security Rule more than the Privacy Rule. Patients whose information was lost or destroyed, and which could have been reasonably safeguarded, could file a complaint with HHS and sue the hospital because important information that may have been, or could be in the future, important to their continuity of care is unavailable.

"There is also the possibility of information that was literally scattered to the winds could fall into the wrong hands and that could bring a claim of violation of the Privacy Rule," she says. "In both of these situations, there would have to be substantiation that the facility did not take reasonable precautions to protect the information."

Such lawsuits are inevitable in the wake of such wide scale data loss, Lyles says, but providers will have a good defense in almost every case.

Risk managers at hospitals throughout the country also have wondered about potential liability risks from the patients transferred for care from the New Orleans area, since many of them arrive without a medical history and unable to describe their past treatment or medications. Treating a patient with so little information may seem like an invitation to liability, but that should not be a problem, Lyles says.

"It sounds like a risky thing, but in reality, this is no different from what every emergency department faces every day if someone is in a car accident and arrives with no history," he says. "They might have a medical record somewhere that says they are deathly allergic to codeine, but you can't be held liable if you had no way to access that information and did the best you could under the circumstances."

The experience of hospitals in the wake of Katrina should be a huge reminder of the need for electronic records in health care, Lyles says. Hospitals would not have lost patient records in the same way if there were electronic records that were backed up off site or accessible through an electronic network, he says. ■

SOURCES

For more information, contact:

- **Kevin Lyles**, Attorney, Jones Day, P.O. Box 165017, Columbus, OH 43216-5017. Telephone: (614) 281-3821. E-mail: kdlyles@jonesday.com.
- **Patricia A. Trites**, Healthcare Compliance Resources, 507 W. Jefferson St., Augusta, MI 49012. Telephone: (800) 973-1081. E-mail: info@complianceresources.com.

HHS issues alert saying HIPAA not a problem

In the midst of Hurricane Katrina, the Department of Health and Human Services (HHS) issued a special alert advising health care workers that were allowed to share protected patient information to provide necessary medical care. The notice also explained that providers were not required to gather patient signatures when sharing information with disaster relief organizations if obtaining the signatures would hinder the disaster response. **(For information on how to access the full HHS bulletin, see resource box on p. 143.)**

Special Report: Lessons from Hurricane Katrina

The Health Insurance Portability and Accountability Act (HIPAA) allows information-sharing to coordinate care with relief workers and to notify family members or responsible parties of a patient's location and general condition or death, the notice explained. It also allows providers to share information with the police and news media for the purpose of locating or identifying responsible parties and allows health care facilities to answer inquiries about whether a patient is at the facility, the patient's location within the facility, and general condition.

These are excerpts from the HHS bulletin

RESOURCE

For the full bulletin on compliance the Health Insurance Portability and Accountability Act (HIPAA) during a disaster, go to www.hhs.gov/ocr/hipaa/KATRINAnHIPAA. pdf.

released on Sept. 2:

"Providers and health plans covered by the HIPAA Privacy Rule can share patient information in all the following ways:

• **Treatment.** Health care providers can share patient information as necessary to provide treatment. Treatment includes sharing information with other providers (including hospitals and clinics), referring patients for treatment (including linking patients with available providers in areas where the patients have relocated), and coordinating patient care with others (such as emergency relief workers or others that can help in finding patients appropriate health services). Providers can also share patient information to the extent necessary to seek payment for these health care services.

• **Notification.** Health care providers can share patient information as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the individual's care of the individual's location, general condition, or death. The health care provider should get verbal permission from individuals, when possible; but, if the individual is incapacitated or not available, providers may share information for these purposes if, in their professional judgment, doing so is in the patient's best interest. Thus, when necessary, the hospital may notify the police, the press, or the public at large to the extent necessary to help locate, identify, or otherwise notify family members and others as to the location and general condition of their loved ones.

In addition, when a health care provider is sharing information with disaster relief organizations that, like the American Red Cross, are authorized by law or by their charters to assist in disaster relief efforts, it is unnecessary to obtain a patient's permission to share the information if doing so would interfere with the organization's ability to respond to the emergency.

• **Imminent danger.** Providers can share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public — consistent with applicable law and the provider's standards of ethical conduct.

• **Facility directory**. Health care facilities maintaining a directory of patients can tell people who call or ask about individuals whether the individual is at the facility, their location in the facility, and general condition. Of course, the HIPAA Privacy Rule does not apply to disclosures if they are not made by entities covered by the Privacy Rule. Thus, for instance, the HIPAA Privacy Rule does not restrict the American Red Cross from sharing patient information. ■

Frequency of med claims falls, while severity rises

While the severity of malpractice claims continues to rise — growing at a rate of 7.5% annually — the frequency of malpractice claims has decreased by 1% over the past year, according to the *2005 Benchmark Analysis: Hospital Professional Liability and Physician Liability* released recently by Aon Risk Consultants in Columbia, MD.

This is the first time in the history of the study the frequency trend decreased in claims for hospitals and physicians, says **Greg Larcher**, assistant director and actuary of Aon Risk Consultants and author of the analysis.

"We believe that legislative reforms in several states over the last few years are contributing to the reduction in claims," he explains. "In addition, the medical malpractice availability and affordability crisis of the last several years has resulted in a rapidly growing alternative market. Health care systems now have a greater financial incentive to reduce their cost of risk."

Larcher also suggests that actions taken by health care systems to improve quality of care and a heightened awareness of how quality care and patient safety tie directly to the cost of risk

COMING IN FUTURE MONTHS

- Condition H protocol reduces fatal errors
- Preventing and responding to sexual misconduct
- Educating physicians about disclosure policy
- Just culture and a progressive accountability model

also have played a role in the decline.

The comprehensive study examines more than 200,000 hospital bed equivalents and represents approximately 10% of the hospital professional liability market and 15% of the alternative segment of the market, making it the largest analysis of its kind, Larcher says. *[Editor's note: The full Aon report is available for purchase. Call (800) 242-2626 and request item 178700. Or go to www.ahaonlinestore.com and enter "178700" in the search box. The cost is $250 for American Hospital Association members and $350 for nonmembers, plus $23.95 shipping and handling.]* ■

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. **The semester ends with this issue.** 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.

21. Who does Kenneth N. Rashbaum, JD, say is responsible for protecting a health care organization from employees seeking to intentionally harm patients?
A. The risk manager is solely responsible.
B. Legal counsel must handle the issue independently.
C. Top administration is responsible, and the risk manager should participate only if explicitly invited to do so.
D. The risk manager may have to take the lead, but human resources and legal counsel must be involved.

22. According to Rashbaum, what is the essence of a "negligent references" claim?
A. The employee says you only gave half of the story and left out information that would have made him or her look better to the new employer.
B. The employee says you should not have given any information about his work history.
C. The employee claims that you provided factually incorrect information about his work history.
D. The employee claims you should have obtained his permission before releasing any information.

23. According to Thomas H. Gallagher, MD, which of the following is true of the physicians he surveyed regarding error reporting in their hospitals?
A. 45% of physicians said they didn't know if their hospital had an error reporting system.
B. 60% were aware of their hospital's error reporting system but had never used it.
C. 70% were aware of the hospital's error reporting system but refused to participate.
D. 85% were aware of the hospital's error reporting system and had reported an error in which they were involved.

24. What does Lori-Ann Rickard, JD, say about the protection offered by Good Samaritan laws for health care workers who go to work in disaster zones?
A. The laws never apply.
B. The laws offer complete protection but only for a very limited time.
C. A Good Samaritan law in the worker's home state provides protection but not a law in the state where the disaster strikes.
D. Good Samaritan laws can protect workers if they volunteer, but not if they will be paid by their regular employers.

Answers: 21. D 22. A 23. A 24. D.

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

Wrong-site surgery results in $455,000 verdict in New York

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

News: A man was diagnosed with a cancerous tumor in his left kidney. After determining that the diseased kidney needed to be removed, an embolization procedure was scheduled to minimize bleeding during the surgery. A radiologist used a fluoroscope, which created a referential image of the patient's kidneys on the screen. As a result of the reversed image, the doctor embolized the wrong kidney. Although the doctor ultimately performed surgery on the correct, left kidney, the interventional procedure performed on the wrong kidney resulted in reduced function. The patient brought suit against the physician who preformed the procedure, the hospital, and the manufacturer of the fluoroscope. The jury found each approximately one-third at fault for the $455,000 verdict.

Background: A 57-year-old man was diagnosed with a cancerous tumor in his left kidney. Before undergoing surgery to have the diseased left kidney removed, doctors scheduled an embolization procedure to control bleeding during the procedure by occluding a problematic blood vessel. The procedure consisted of injecting foam into the relevant artery to halt blood flow to the kidney, thus minimizing blood loss during the kidney's removal.

An interventional radiologist performed the embolization with a fluoroscope, an instrument consisting of an X-ray machine and a fluorescent screen to observe the size, shape, and movement of the patient's blood vessels during the procedure. Using the fluoroscope to locate what the doctor thought to be the left kidney and relevant artery, the radiologist commenced the embolization. Unfortunately, however, the fluoroscope had erroneously created a reverse image of the patient's kidneys on its screen, leading the radiologist to begin the procedure on the patient's *right* side. The procedure was halted when the patient complained of pain on his right side. The physician immediately realized that he had begun to embolize the wrong kidney.

It took four days of hospitalization for the patient's right kidney to stabilize. His tumorous left kidney was subsequently embolized and removed. The patient claimed that his remaining right kidney had been permanently damaged and its function was decreased significantly. He also contended that he has experienced significant distress stemming from his concern regarding his remaining kidney's health. His expert urologist added that as a result of the compromised kidney, he might require dialysis in the future.

The patient brought suit against the radiologist, the hospital, and the manufacturer of the fluoroscope. His wife also joined the suit and claimed loss of services. Testimony indicated that the fluoroscope had a history of image-reversal malfunctions and that the physician performing the wrong site procedure already had experienced at least

one prior instance of this particular imaging device malfunctioning in this manner. As it turns out, the hospital staff also were aware of the malfunction and had made several service calls to the manufacturer, but the staff failed to provide evidence that they had warned the radiologist of the situation. The plaintiff produced hospital maintenance records, which showed that the machine had malfunctioned on numerous occasions and that the manufacturer had failed to fully repair the device. The plaintiff maintained that even in the absence of the warning by staff, the treating physician should have taken extra precaution to ensure that the embolization was performed on the correct kidney. The patient argued that such precautions could have been affected through the use of markers or other visual aids.

As for the manufacturer of the fluoroscope, the plaintiff claimed that the company had knowingly produced and marketed a defective fluoroscope and that the company's service crew was negligent for failing to have properly diagnosed and repaired the fluoroscope's repeated malfunction.

The physician contended that the standard of care did not require that he use markers prior to an embolization because the orientation of the patient was checked at the beginning of the procedure. He also added that he did not "expect" the fluoroscope to malfunction. The hospital tried to affix blame on the manufacturer for failing to fix the device when they had repeatedly requested them to do so. The manufacturer countered with the notion that the image reversal was not an inherent problem with the device, but rather it was an operator error.

The jury found the radiologist liable for 30% of the damages and the hospital and manufacturer each 35% liable. The jury awarded the patient and his wife a total of $455,000. The patient received $150,000 for past pain and suffering and $250,000 for future pain and suffering; his wife received $55,000 for past and future pain, suffering, and loss of services.

What this means to you: Wrong-site surgery is one of the gravest issues facing risk managers, practitioners, and facilities. "Despite increased awareness, preventive recommendations, zero tolerance on behalf of health care facility and practitioner regulators, wrong-site, wrong-person, or wrong-procedure surgery remains the close second leading sentinel event reported to the Joint Commission on Accreditation of Healthcare Organizations [JCAHO] by general hospitals," states **Leilani Kicklighter,** RN, ARM, MBA, CPRHM, director of risk management services and patient safety officer at Miami Jewish Home & Hospital for the Aged in Miami and past president of the American Society for Healthcare Risk Management. "There is the pervasive belief that these occurrences simply should never happen, but in reality, we should never say 'never,' but we should endeavor to prevent such occurrences."

"A root-cause analysis, of course, must be done whenever such incidents occur, as these are JCAHO reportable sentinel events," notes Kicklighter.

"The JCAHO summary data from reported sentinel events reflects that communication is the leading contributory factor, and there was certainly a great lack of communication among the providers in this case," she adds.

The facts of this case generate an abundance of questions. "According to the facts of this case, there was a known history of the reversing images when using this particular fluoroscope. This raises several issues. First, to whom were these prior incidents reported? Second, what was done about these recurring errors? Finally, was this ever reported under the Safe Medical Device Act [SMDA] to the Food and Drug Administration [FDA] and the manufacturer? Since this was a known recurring error, why was the fluoroscope allowed to remain in service? Why weren't the interventional radiologists ever advised of this recurring error?" queries Kicklighter.

"What all this boils down to is a question of where risk management was in this situation before this final incident. Why was this piece of equipment allowed to remain in service?" asks Kicklighter. "Reporting under the SMDA is a collaborative effort between biomedical/materials management and risk management with the 'buck stopping' at risk management. Risk management should oversee the education of all employees and physicians regarding their role in the identification, tag out and lock out, and reporting of any piece of equipment that malfunctions, even if it is due to 'user error.' Incident reports of malfunctioning equipment should be reported to risk management just like any other unusual event."

Unfortunately, this piece of machinery remained in circulation, and processes were not in place to counter its use. "In view of the fact that this equipment had been sent to the manufacturer for repair but was not actually repaired, risk management should have been more involved with the FDA and the manufacturer to be sure the equipment was indeed repaired. If the manufacturer's feedback

was that it was 'user error,' risk management and biomed should have initiated educational sessions with the manufacturer's representative and the users of the equipment to overcome that user defect. As it was, physicians and staff just kept using it," observes Kicklighter.

In 2004, the Joint Commission listed wrong-site surgery among its principal safety goals and suggested that facilities create and use a preoperative verification process, such as a checklist, to confirm that appropriate documents — including medical records and imaging studies — are available to the surgical team. In addition, the Joint Commission recommended that providers implement a process to mark the surgical site and, to the extent possible, involve the patient in the marking process.

The Joint Commission also has approved a universal protocol for preventing wrong-site, wrong-procedure, and wrong-person surgery. The principal components include the preoperative verification process, marking of the operative site, taking a "time out" immediately before starting the procedure, and adapting the requirements to nonoperating room settings, including bedside procedures.

"It would appear that this unfortunate outcome was not the usual wrong-side or wrong-site surgery scenario that would have been avoided by using the time out or marking of the proper site, since this was an error caused by a flipping of the fluoroscopy visualization. Although preoperative, or in this case pre-procedure, verification and perhaps even earlier patient involvement may have been beneficial, this makes it all the more critical that compliance with the SMDA process is revisited and implemented with frequent reinforcements. It would appear that the root cause of this untoward outcome was failure to communicate among all the parties who were in any way involved with this equipment on all levels, which as noted earlier is the most common element in wrong-site incidents," concludes Kicklighter.

Reference

- Queens (NY) Supreme Court, Index No. 22859/95. ■

Misplaced dead body, $17,550 Nevada verdict

News: A patient died of natural causes at the defendant hospital. However, when the funeral home came to collect the body, it took the hospital 2½ days to find the corpse. At that point, the decedent had to be cremated, which was against his religious preference. The man's children brought suit, and each received $5,850.

Background: The plaintiffs' father died of natural causes in the defendant hospital after undergoing an angioplasty to open narrowed coronary arteries. There were no issues regarding the appropriateness or adequacy of medical care and treatment he received. However, when the plaintiffs went to retrieve the body the next day, hospital officials told them that they could not find a record for their father in the computerized record system. The hospital instructed the plaintiffs to contact a local funeral home that typically handled deceased bodies from the hospital. When the funeral home told the plaintiffs that the corpse was not there, the plaintiffs demanded that the hospital find their father's body.

After 2½ days of searching, the decedent's body was located in the hospital's basement. After the man's death, hospital workers had placed the body on a gurney under a tabletop, enclosed by steel walls in an effort to hide the corpse while wheeling it through hallways. All that can be seen when the cart is wheeled down the hall is something that looks like a large serving cart with a floor-length sheet draped over its sides.

Unfortunately, a shift change caused a mix-up in keeping track of the body. The personnel leaving failed to tell the incoming workers where the decedent's body had been put. As a result, the hidden body sat on the gurney in a hallway for at least a day before it was moved to a warm, locked room in the basement.

The high temperature and lack of fresh air for 2½ days caused the body to decompose. It could be identified only by a tattoo on the decedent's arm. The plaintiffs contended that the body, in its present state, could not be embalmed or transported home to Utah. Instead, the remains had to be cremated, a process that was against the family's religious beliefs and that prevented a viewing of the body.

The hospital successfully argued that the misplacement of the body was partially a result of the plaintiffs' failure to make timely funeral

arrangements. A verdict of $6,500 was awarded to each of the decedent's three children; however, since the children were found be 10% at fault, the award was reduced accordingly.

What this means to you: "One of the most difficult situations a family faces is the death of a loved one," says **Cheryl Whiteman**, RN, MSN, HCRM, clinical risk manager for Baycare Health System in Clearwater, FL. "Even when death is expected, the reality of their loss can be harsh and difficult to endure. One way societies deal with this loss is through the meaningful rituals, dictated by culture, religious beliefs, or both. In this situation, the family most likely experienced justifiable anger when the facility misplaced the body of their loved one. While the family may have contributed to the situation by not making funeral arrangements in a timely fashion, this is something that health care facilities should anticipate."

"Whether articulated in a mission statement or understood through the tradition and basic premises of health care, the dignity and respect of the individual should be maintained at all times."

The Joint Commission on Accreditation of Healthcare Organizations addresses the treatment of dying patients by noting that the "social, spiritual, and cultural variables that influence the expression and perception of grief by family members should be attended to."

Notes Whiteman, "The strain that illness and death causes often prevents people from being able to make decisions. This can be compounded if there are differences of opinions between family members."

"Whether articulated in a mission statement or understood through the tradition and basic premises of health care, the dignity and respect of the individual should be maintained at all times. Caring for the individual throughout the continuum should, indeed, include respectful attention to the remains of the deceased, including safely relinquishing the body to the appropriate funeral home or agency," emphasizes Whiteman.

"The risk manager should have been engaged in two processes, either directly or indirectly. First, a massive search should have been undertaken to locate the body in significantly less time than 2½ days. This search should have been similar to the process utilized in locating a missing patient. The entire hospital staff should have been alerted. Finding a decomposing body would be quite shocking to unsuspecting staff, visitors, or another patient," says Whiteman.

"And secondly, risk management should have been involved in dealing with the concerns of the family, including offers to assist with the financial burden of funeral expenses and perhaps family travel. Certainly financial expectations may escalate in view of the fact that religious beliefs, which often become paramount at such a time, were violated when the body had to be cremated. In the absence of extreme financial demands from the family, it seems that this issue should have been resolved outside of the courtroom. It would be expected that during the litigation process, the family would have many opportunities to express their outrage to others. The impact of this story would likely be passed through many, many people throughout the community, undermining the credibility of the health care facility," adds Whiteman.

"After locating the remains and rectifying the situation as much as possible, the risk manager would need to conduct an analysis of how the body happened to be 'lost' and to make appropriate process changes to prevent this situation from reoccurring," concludes Whiteman.

Since the incident, the hospital has instituted new policies for keeping track of the deceased. One new policy mandates that if relatives of the deceased cannot be notified within eight hours of the patient's death, the hospital must send the body to the mortuary in rotation. That information is logged into the computerized record system so that family members can locate their deceased loved ones when contacting the hospital. The second new policy requires workers to notify a nursing supervisor whenever a deceased person's name is deleted from the computer system. As a result, when family members call the hospital looking for information about their deceased loved ones, those calls can be routed to the appropriate supervisor, who can inform the relatives of the body's whereabouts. By implementing these new policies, the hospital in this case avoided any fines or penalties from the state health division.

Reference

• Clark County (NV) District Court, Case No. CV A446403. ■

Healthcare Risk Management™

2005 Index

When looking for information on a specific topic, back issues of *Healthcare Risk Management* may be useful. If you haven't already activated your on-line subscription so that you can access the newsletter archives through the company web site, just click the "Activate Your Subscription" button in the left navigation area of www.ahcpub.com. Or contact our customer service department at P.O. Box 740060, Atlanta, GA 30374. Telephone: (800) 688-2421 or (404) 262-7436. Fax: (800) 284-3291 or (404) 262-7837. E-mail: ahc.customerservice@thomson.com.