Healthcare Risk Management™

November 2010: Vol. 32, No. 11
Pages 121-132

IN THIS ISSUE

Financial Disclosure: Author Greg Freeman, Managing Editor Karen Young, Executive Editor Russ Underwood, 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.

RM says she was fired for reporting EMTALA violation

Suing the hospital after dismissal on day CMS investigators arrived

An experienced risk manager says she was fired by her hospital for reporting an Emergency Medical Treatment and Active Labor Act (EMTALA) violation after hospital executives discouraged reporting it for fear of a large penalty. She is now suing the hospital, which denies her allegations.

Margaret O'Connor, RN, was the risk manager at Jordan Hospital in Plymouth, MA, until her firing on May 19, 2010. She had been employed by Jordan Hospital for 38 years, working in various positions related to quality control before becoming risk manager, according to the complaint filed in the U.S. District Court, District of Massachusetts. The claim indicates that O'Connor received an exemplary performance review from her supervisor on November 10, 2009. She reported to Harvey Kowaloff, MD, head of clinical reliability.

O'Connor claims in her lawsuit that she was fired for her actions after an incident at the hospital on March 26, 2010, involving a patient in labor who was transferred to another hospital. Soon after the transfer, O'Connor received a call from the other facility's risk manager, who expressed surprise that the patient had been sent over in active labor and suggested that Jordan Hospital had violated EMTALA, O'Connor says in her lawsuit. The hospital had never before reported an EMTALA violation or been investigated for one. (*See the story on page 123 for more details of the incidents*

EXECUTIVE SUMMARY

A risk manager was fired from her hospital after reporting an EMTALA violation. She claims the firing was retribution for making the report, which hospital executives feared would result in a significant fine.

- The hospital denies she was fired for reporting the EMTALA violation.
- The risk manager is suing her former employer.
- ASHRM says professional intimidation is a serious problem.

AHC Media LLC

that O'Connor says led to her firing.)

O'Connor responded by conducting a full investigation and concluding that Jordan Hospital had violated EMTALA, the claim says. When she reported her findings to senior management, she indicated that she planned to notify CMS immediately, because the law required her to do so and because the hospital would fare better if it self-reported, rather than risking that the other facility would report the incident. According to O'Connor, her boss, Kowaloff, discouraged reporting.

She reported the EMTALA violation to CMS, which prompted an investigation of the hospital. The investigators concluded that Jordan Hospital had violated EMTALA four times in addition to the one reported by O'Connor. The potential penalty was a total of $250,000.

O'Connor informed hospital management that she intended to notify the patient of the EMTALA violation once the hospital completed a validation survey required by CMS, an extensive process that threatened to find more problems that could lead to more penalties, the claim states. On May 19, 2010, 12 CMS regulators arrived to survey the hospital, and O'Connor was fired the same day. Kowaloff told her the reason was "regulatory," according to O'Connor.

O'Connor referred all questions to her attorney, **Jared Burke**, JD, of Needham, MA.

Christopher Smalley, director of strategic marketing and communications at Jordan Hospital, tells *Healthcare Risk Management* that the hospital flatly denies O'Connor's claims. She was not fired for reporting the EMTALA violation, but the hospital cannot discuss the true reason for her firing because of the ongoing litigation, Smalley says.

"The allegation is false," Smalley says. "I can't get into why she was fired, but as it relates to the allegation of whistleblowing, it had nothing to do with that."

EMTALA specifically prohibits adverse action against whistleblowers. Subsection (i), "Whistleblower protections," states a hospital "may not penalize or take adverse action against a qualified medical person described in subsection (c)(1)(A)(iii) or against any hospital employee because the employee reports a violation of a requirement of this section." CMS did send investigators to the hospital on September 1 to conduct a complaint survey prompted by O'Connor's claim of retribution, but Smalley says they sided with Jordan Hospital.

On September 9, Jordan Hospital received a letter from CMS, which stated that it had investigated allegations of violation of subsection (i) regarding adverse action against a whistleblower and the hospital had been found to be in compliance, Smalley says. Jordan Hospital considers that firm evidence that O'Connor was not fired for whistleblowing, he says.

However, Burke says the CMS investigators did not speak with O'Connor to hear her side

Healthcare Risk Management® (ISSN 1081-6534), including HRM Legal Review & Commentary™, is published monthly by AHC Media, LLC, 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, (customerservice@ahcmedia.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), $499. Add $17.95 for shipping & handling. Outside U.S., add $30 per year, total prepaid in U.S. funds. For approximately 15 CE nursing contact hours, $545. Discounts are available for group subscriptions, multiple copies, site-licenses or electronic distribution. For pricing information, call Tria Kreutzer at 404-262-5482. 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.)

Address: P.O. Box 740056, Atlanta, GA 30374. Telephone: (800) 688-2421. World Wide Web: www.ahcpub.com.

AHC Media LLC is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation.

This activity has been approved for 15 nursing contact hours using a 60-minute contact hour.

Provider approved by the California Board of Registered Nursing, Provider #14749, for 15 Contact Hours.

This activity is valid 24 months from the date of publication.

Healthcare Risk Management® is intended for risk managers, health system administrators, and health care legal counsel.

Opinions expressed are not necessarily those of this publication. Mention of products or services does not constitute endorsement. Clinical, legal, tax, and other comments are offered for general guidance only; professional counsel should be sought for specific situations.

Editor: Greg Freeman, (770) 998-8455.
Managing Editor: Karen Young (404) 262-5423 (karen.young@ahcmedia.com).
Executive Editor: Russ Underwood (404) 262-5521 (russ.underwood@ahcmedia.com).
Production Editor: Neill L. Kimball.

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

of the story. They asked to, he said, but Burke declined their request to speak with his client, because he "didn't know their motivation or what they were seeking."

No coincidence, lawyer says

O'Connor's attorney says there was no other reason to fire the risk manager.

"It's our viewpoint that there was a direct correlation with the timing of her firing and the investigators from CMS coming in. It seems a little too coincidental," Burke says. "She worked there for 38 years, and if you go through her file, she has, I think, one citation. For 38 years, there's nothing, and then to have this happen on the same day investigators come in, obviously there's some animus and retaliatory action."

Burke says neither he nor O'Connor knows what Kowaloff meant when he said the cause of her firing was "regulatory." O'Connor is currently unemployed and seeking another position.

If O'Connor's claims are true and the hospital did fire her for reporting the violation, the hospital could be in for far more trouble than it was already in, says **Matthew Curley**, JD, and attorney with Bass, Berry & Sims in Nashville, TN, who represents clients involved with government investigations.

"The allegations are certainly startling, on the face of the complaint," Curley says. "The law goes to great lengths to protect whistleblowers. The Jordan Hospital case certainly serves as an important reminder to providers to avoid retaliating against employees who report EMTALA violations."

In addition to any settlement or award to O'Connor, Jordan Hospital faces damage to its reputation in the community, Curley notes.

There are generally two key issues in fraud and abuse whistleblower lawsuits, Curley says. First, courts will ask whether there was an underlying violation of the law reported by the whistleblower. Second, courts will examine whether the employer can show that the employment decision at issue was independent of the whistleblower's reporting of the issue.

Disputing the underlying violation of the law would be exceedingly difficult, because CMS determined there had been a violation, Curley notes. That leaves the hospital's only avenue of defense to be claiming that O'Connor was fired for something unrelated to reporting the EMTALA violation, he says. Any documentation showing the fired employee had previous or ongoing problems with work quality would help the hospital, but lacking that, simply saying there was a legitimate reason for the dismissal probably won't be received well, he says.

"If we assume the facts in this complaint, the hospital will certainly have a challenge in defending this lawsuit," Curley says.

SOURCES

• **Jared Burke**, JD, Law Offices of Timothy M. Burke, Needham, MA. Telephone: (781) 455-0707. E-mail: burkejared@gmail.com.
• **Matthew Curley**, JD, Bass, Berry & Sims, Nashville, TN. Telephone: (615) 742-7790. E-mail: mcurley@bassberry.com. ■

Lawsuit claims RM acted appropriately

Editor's note: Healthcare Risk Management *summarizes here the points made in a risk manager's case against her former employer, Jordan Hospital, which vehemently denies that her firing earlier this year was related to whistleblowing. However, we provide this information to offer one person's view into the inner workings of hospitals.*

The lawsuit filed recently by **Margaret O'Connor**, RN, the risk manager at Jordan Hospital in Plymouth, MA, until she was fired recently after reporting an EMTALA violation, outlines what she says was an act of retaliation by hospital leaders.

After her dismissal, O'Connor sued the hospital, the board of directors, President and CEO Peter Holden, Vice President of Organizational Development William Kirkwood, and Head of Clinical Reliability Harvey Kowaloff, MD. *Healthcare Risk Management* obtained a copy of the complaint filed against the hospital, and this is how she describes the events that she says led to her firing:

• About 8 a.m. on March 26, 2010, a patient came to the emergency department. She was six months pregnant with twins, diabetic, and considered a high-risk pregnancy. She complained of abdominal pain and nausea. A nurse practitioner diagnosed a "stomach bug" and ordered intravenous fluids but no further testing, observation, treatment, or diagnosis. The patient actually was in active labor.

• After two hours, during which the patient continually complained of abdominal pain, the nurse practitioner determined that the patient was in labor. At this time, the patient asked to be transferred to South Shore Hospital in Weymouth, MA. She was transferred at 10:20 a.m. without approval from an attending physician. No physician had determined she was in stable condition and safe to transfer.

• The leg of one her twins was protruding into the patient's vagina when she arrived at South Shore. Both premature babies were delivered by emergency caesarian section. The mother suffered a partial abruption of the placenta. The second child experienced significant complications, including ingestion of blood into the lungs, and required intubation and a respirator.

• Two days later, O'Connor received a phone call from the South Shore risk manager, who said she was very concerned with the transfer. She said "Do you people have doctors over there? I hope this isn't an EMTALA violation." O'Connor had no knowledge of the incident at that point, but she told her South Shore counterpart that she would investigate and get back to her.

• O'Connor investigated the incident and determined that the transfer violated EMTALA. She reported the violation to senior management.

• O'Connor consulted Jordan Hospital's legal counsel, who advised her to self-report the violation as mandated by the CMS Conditions of Participation. Counsel also advised that it would be better to report the violation before South Shore reported it.

• She met with Kowaloff, Holden, and Deborah Sullivan, senior director of clinical reliability and patient safety officer. O'Connor discussed the incident, why it was reportable, and the potential penalties. During the meeting, Kowaloff went on the Internet and determined that the hospital would face a $50,000 fine. Holden, the president and CEO, told O'Connor that he was "not telling you not to report it, but let's make sure we need to."

• O'Connor explained that the hospital was required by law to report the violation, and the hospital attorney advised reporting it. She also explained that the hospital would be at greater risk if South Shore reported it first.

• O'Connor then solicited help from the hospital attorney to summarize the events and complete the report. She then met with Sullivan and Kowaloff to complete the action plan and obtain senior management's approval before making the report. Then O'Connor contacted the South Shore risk manager to advise that Jordan Hospital was self-reporting.

• O'Connor submitted the report to CMS. Three days later, Jordan Hospital was visited by the Department of Public Health, which investigates EMTALA violations on behalf of CMS. The department's five-day investigation found multiple violations in obstetrics and the emergency department. The investigators concluded that there had been as many as four prior EMTALA violations, in addition to the one reported. The potential penalty would be $250,000.

• The report also outlined major deficiencies in education of staff regarding EMTALA, hospital policies not in place or not followed, signage not available, and failure to educate patients about the risks of transfers. O'Connor began working on remedies to the problems cited.

• CMS informed Jordan Hospital that the EMTALA violation required the hospital to complete a validation survey from CMS, which senior management knew would be intensive and likely to result in more citations and penalties.

• Before that survey began, a department director asked O'Connor why she had to report the violation when the mother and twins were doing well. O'Connor informed senior management that she planned to also inform the patient of the violation after the CMS validation survey was complete.

• On May 19, 2010, 12 CMS investigators arrived to conduct the validation survey. The same day, shortly after their arrival, O'Connor was called to a meeting with Kirkwood and Kowaloff, where she was fired. Kowaloff told her the reason was "regulatory." ■

ASHRM stands behind fired risk manager

Retaliatory firing of a risk manager for reporting regulatory infractions is outrageous but not unheard of, says **Dan Groszkruger**, JD, MPH, CPHRM, DFASHRM, risk manager at Stanford (CA) University Medical Center and a board member of the American Society for Healthcare Risk Management (ASHRM) in Chicago.

Speaking on behalf of ASHRM, Groszkruger says the case of Margaret O'Connor, the risk manager suing her former employer for what she says was retribution after reporting an EMTALA

violation, is troubling. Groszkruger acknowledges that O'Connor's complaint is only one side of the story, and Jordan Hospital has not been proven to have fired her for whistleblowing. Nevertheless, he says the scenario outlined in O'Connor's complaint is believable, and she wouldn't be the first risk manager punished for doing her job.

"I can verify based on my own personal experience that this is not exactly unusual," Groszkruger says. "One task of the risk manager is to protect the organization's resources and finances, and the mandatory reporting scenario is almost bound to do harm to that. It's a potential conflict, because the risk manager has to wonder if they're going to shoot the messenger."

Groszkruger notes that once the EMTALA violation occurred, it appears O'Connor did all the right things and even went further than strictly necessary to confirm that the case was reportable, he says.

"If her allegations are all provable and factual, she really got the shaft for doing the right thing," he says. "Reading the complaint and assuming this to be an accurate description, we would find someone who was terminated for doing this to be appalling, just about as troubling and worrisome as anything you could imagine. If indeed the decision to terminate was based on going ahead and reporting this, it's wrong. It's absolutely wrong."

Groszkruger says the description of the patient provided by O'Connor suggests she was right in concluding that the incident was a reportable EMTALA violation.

"I certainly couldn't see anything based on these allegations that would lead you in a different direction," he says. "It's almost an obvious violation."

ASHRM has been focusing more on professional intimidation, Groszkruger says, trying to offer its members support or advice when placed in these difficult situations. Much of the intimidation is less direct than firing or any overt punishment, he says.

"A lot of it is along the lines of 'I'm going to make your life miserable if you report me on this,'" he says. "It interferes with transparency and disclosure to the patient and family, let alone turning yourself in to regulators."

Groszkruger urges risk managers to turn to their colleagues in the field when faced with professional intimidation, partly to realize that they are not alone in facing such a dilemma and partly to seek advice on how to respond. ASHRM encourages risk managers to take the high road even when pressured, he says.

"I don't think this kind of conflict is something on which you can waver," Groszkruger says. "We're talking about what's right and wrong, what is honest or dishonest, what is the truth or a lie. When you get into that category, you're talking about integrity and self-respect."

SOURCE

• **Dan Groszkruger**, JD, MPH, CPHRM, DFASHRM, Risk Manager, Stanford (CA) University Medical Center. Telephone: (650) 725-4061. E-mail: dgroszkruger@stanfordmed.org. ■

Fake mammogram results lead to indictment

A hospital in Georgia is facing many questions after a former employee was indicted for what authorities say was intentional fraud in entering negative results for mammograms that, in fact, had not been read by a radiologist.

A former hospital employee in Perry, GA, was indicted recently on 10 felony counts of computer forgery and 10 counts of misdemeanor reckless conduct, with prosecutors alleging that she entered negative results for 1,289 mammograms at Perry Hospital, says **Jason Ashford**, JD, chief assistant district attorney for Houston County.

"At this point we know of 10 victims, but there could be more," Ashford says.

The indictment against 30-year-old radiology technician Rachael Michelle Rapraeger was announced at a news conference at the District Attorney's Office at the Houston County Courthouse in Perry. The district attorney said the fake results were entered from Jan. 22, 2009, to April 1, 2010. Ashford says that when radiologists did examine the mammograms, 10 of them actually were positive, and those are the cases in which Rapraeger has been charged. Ashford said that Rapraeger is believed to have acted alone and

EXECUTIVE SUMMARY

A radiology technician has been indicted for allegedly faking negative results for 1,289 mammograms over about 15 months. The hospital fired her when the false results were discovered and is now facing questions about how the alleged fraud could have gone on so long.

- The hospital discovered irregularities in records and then conducted an investigation.
- No others have been accused of participating in the alleged fraud.
- The hospital is likely to face malpractice suits and regulatory action.

without the knowledge of any radiologist or other physician.

The computer forgery charges carry a maximum penalty of 15 years each, and the reckless conduct charges carry a maximum of one year each.

"So, we're talking a total of 160 years potentially," Ashford says. Ashford was unable to comment on Rapraeger's alleged motive, because the investigation is ongoing.

"At this point we believe she acted alone; however, we are not just assuming that," he says. "We do not have any indication at this point that she acted in conjunction with anyone else, but we'll see where the investigation goes — and if it leads us to anybody else who was involved."

Victor Moldovan, JD, an Atlanta attorney representing Houston Healthcare, which operates Perry Hospital, issued a statement saying an anomaly in patient records was discovered April 2, and as hospital officials investigated, a technician admitted on April 5 that she signed off on mammograms as if she were the radiologist. The woman, now identified in the indictment as Rapraeger, was sent home that afternoon and dismissed April 6, he said.

The hospital's internal investigation was triggered in part by a quality check, according to **Ashley Harris**, Moldovan's assistant. The total number of mammograms performed during that time period has not been divulged, she says, so it is not known what percentage of all the mammograms is represented by the number alleged to have been forged.

"The number being focused on is the 1,289 patients impacted by this former employee, and we are communicating with these individuals and their physicians," she says.

The hospital issued a statement confirming the incident but declined further comment. (*See the story on page 127.*)

More problems coming

Part of the problem may be that radiology technicians at most hospitals have a great deal of autonomy, says **Susan Friery**, JD, MD, an attorney with the law firm of Kreindler & Kreindler in Boston. They work with the patient to obtain the mammogram image and then send the file to a radiology group for review, she says, and those radiologists usually are contracted physicians, rather than hospital employees.

That same employee often does the billing, as well, which creates an opportunity for fraud, because there is little oversight or involvement of others, she says. What she finds curious is that the radiologists apparently never noticed they were making less on mammograms and discovered the fraud that way.

Within the hospital, Friery questions how the fraud could continue for so long without anyone noticing what must have been discrepancies in the documentation. For instance, the radiologist would have to dictate notes and indicate by signing that he or she had read them. Were the documents just not signed, Friery wonders. Or did the tech fake signatures as well?

"The standard of care does not require that the hospital go through every radiology report every month to make sure everything is done correctly," she says. "I will say, however, that the hospital [is] required to be sure that the reports are signed."

Checks and balances needed

It is possible for a radiology tech to skim a few patients at a time, rather than faking results for all mammogram patients, Friery notes. Perhaps the tech wants to lighten the workload a bit or speed up the dispensation of cases at the end of the day, so he or she just fakes the negative result for some portion, according to Friery. That kind of fraud can be avoided by coordinating with the radiology group and requiring accountability, she says.

"There should be a policy that you tell the radiologist how many patients you are seeing that day, and then the radiologist should make sure the numbers match at the end of the day," Friery says. "If they were told 32 patients, and they've only seen 24, they should ask what happened to those other eight patients. There should be a check and balance."

The hospital could be sued for negligent hiring and negligent supervision, Friery says, along with not having the proper protocols and monitoring in place to prevent the fraud or detect it sooner. She expects Perry Hospital to be inundated with malpractice cases as a result of the mammogram fraud, but she says plaintiffs will have to prove that a delayed diagnosis actually caused harm.

"Unless it changed the course of the disease, like showing that you could have had a lumpectomy but now you have to have a mastectomy, the plaintiff won't have much of a case," she says. "An emotional lawsuit based only on the shock of realizing you had cancer for two years but never knew

it won't go very far. Some juries will say you were lucky not to have to worry about it for two years."

More cases than reported?

The hospital most likely will claim that the radiology tech was a rogue employee who willfully disobeyed hospital policies and procedures, says **Nadeem Bezar**, JD, an attorney with the law firm of Kolsby Gordon in Philadelphia. Nonetheless, he thinks Perry Hospital is in deep trouble.

"The exposure for the hospital is tremendous, and it's almost disastrous. We're . . . talking about close to 1,300 mammograms, and that's about 100 mammograms a month or three per day," Bezar says. "There absolutely is groundwork for medical negligence, and it's going to be more than 10 people."

Bezar questions the report that only 10 of the fake negative mammogram results were found to be positive.

"I would suggest that is inaccurate," Bezar says. "The abnormal findings rate for mammograms hovers around 6% to 8%, so we're talking about more like 80 or maybe even 100 abnormal findings should turn up, of which a high number of those could be cancerous lesions. That's it's only 10 is astounding. I'm going to guess that the hospital is underreporting."

The modern way of reading mammograms may increase the hospital's exposure, Bezar says. Rather than the old way of putting a film up on a light box to read, mammograms are now sent digitally to the physician, who can access it only by entering a unique code. That code allows the hospital to track who has viewed the file and when, Bezar says.

The system prevents a tech from entering information in the doctor information areas, so faking a result in the digital system would mean the tech had access to the doctor's identification number. Whether the tech stole it or was given the number would be an important question, he says.

Friery agrees, saying that if a tech obtained that data on a number of radiologists and used them all for fraudulent billing, that is a concerted effort to hide her work. But if she used one doctor's name and identification over and over again, that is another red flag that should have alerted the hospital to trouble.

"I think there's going to be a regulatory problem for the hospital. I'd be asking how a radiology tech could get access to the physician codes, why you didn't have the records cross referenced, why you didn't have checks and balances that discovered this before it went on so long," Bezar says. "Did you have a system that flagged things like a physician signing off on a film when he wasn't even signed into the system? The hospital is going to have to answer some hard questions."

SOURCES

- **Susan Friery**, JD, MD, Partner, Kreindler & Kreindler, Boston, MA. Telephone: (212) 687-8181. E-Mail: sfriery@kreindler.com.
- **Nadeem Bezar**, JD, Partner, Kolsby Gordon, Philadelphia, PA. Telephone: (212) 851-9700. ■

Hospital confirms results were faked

The employee in question is still facing criminal charges, but Perry (GA) Hospital has confirmed that a technician faked mammogram results.

After the indictment, Cary Martin, interim chief executive officer for Houston Healthcare System, Inc., the parent company of the hospital, issued a statement confirming the fraud. On the day of the indictment, Martin's statement noted that the district attorney concluded that former Perry Hospital employee Rachael Michelle Rapraeger acted alone.

"Perry Hospital has completed its own internal review of the radiology department and also concluded that Ms. Rapraeger acted alone," Martin said. "Perry Hospital supports the district attorney's decision to proceed with a criminal indictment."

Martin said Perry Hospital is thoroughly cooperating with the Perry police department and the Houston County district attorney in identifying all patients who were potentially impacted by Rapraeger's alleged actions.

"Although our initial estimate was that approximately 900 patients were impacted, after a complete and thorough investigation, we concluded that an additional 389 patients could have been affected by her actions. We have taken steps to locate and notify each of these patients," Martin said. "We at Perry Hospital and Houston Healthcare sincerely regret the actions of Ms. Rapraeger and the consequences such actions have brought by her unauthorized and inexplicable acts; however, due to patient confidentiality and the ongoing criminal investigation, we cannot publicly address specific patients. We are working to communicate with all impacted patients. The

Hospital's commitment to patient care remains its primary focus, and we will continue to work to address any concerns patients may have."

The hospital provided a hotline number for patients to call if they were concerned that their mammogram results were involved. ■

Johns Hopkins shooting shows need to prepare

A recent shooting incident at Johns Hopkins Hospital in Baltimore shows the need to prepare for gun violence, but it also illustrates the limitations of any prevention program, security experts say.

Fifty-year-old Warren Pardus was speaking with the surgeon treating his mother when he pulled out a semiautomatic pistol and shot the doctor in the abdomen, according to reports from the Baltimore Police Department. He then ran into his mother's room, and the immediate area of the hospital was evacuated, police say. After a two-hour wait, a police robot entered the room and found Pardus and his mother dead from gunshot wounds.

The surgeon, David B. Cohen, MD, underwent emergency surgery for a gunshot wound to his abdomen, and Johns Hopkins reported he was in stable and fair condition the next day. Cohen is an orthopedic surgeon specializing in spinal work. Witnesses told the *Baltimore Sun* that he had been discussing the 84-year-old mother's prognosis when Pardus yelled, "You ruined my mother," before shooting. Witnesses told the newspaper that the mother had been left paralyzed after surgery intended to make her more mobile. *(For the Baltimore Sun report, go to http://articles.baltimoresun.com/2010-09-17/news/bs-md-ci-shooting-hopkins-20100916_1_mother-hospital-staff-east-baltimore.)*

EXECUTIVE SUMMARY

A patient's relative shot a physician at Johns Hopkins Hospital in Baltimore creating a crisis and police response. The man killed his mother and himself soon after shooting the doctor.

- Security experts say Johns Hopkins responded well to the incident.
- The hospital was able to isolate the problem to a relatively small area.
- Johns Hopkins used social media to alert staff to the hazard.

A spokesman from Johns Hopkins declined comment because of the ongoing criminal investigation.

More incidents to come?

Risk managers can expect to see more such incidents in the future, says **Sean Ahrens**, CPP, BSCP, CSC, senior security consultant with Schirmer Engineering in Glenview, IL.

"With the increased pressure being put on emergency departments and the increased stress that people feel from a variety of factors, we may be seeing more situations in which people lose control of themselves and act out violently," he says. "This isn't going to happen every day, but it has always been a problem in health care facilities; and I'm afraid it's going to get worse in the near future."

In many ways, the shooting was typical of how gun violence happens in a health care setting, says **Timothy Dimoff**, CPP, founder and president, SACS Consulting and Investigative Services, Akron, OH. It is common for violence to be precipitated by patients or family members receiving bad news, and those situations should always be assessed carefully, he says.

"There are cases where you can identify that you have the potential for a violent situation, whether it is with a gun or with a violent outburst. When that happens, then you can start notifying security that you have a situation where someone is upset," he says. "You need training for hospital staff and physicians, so that they can try to recognize those situations before it escalates."

Good response at hospital

Johns Hopkins apparently did a good job isolating the situation so that no other staff and patients were at risk, Dimoff says. He sees two lessons to be learned from the Johns Hopkins incident. First, he says it is a reminder that hospitals should train staff to help recognize disgruntled patients who could become violent. Verbalizing their anger, by shouting or raising their voices, is an important warning sign, Dimoff says.

The second lesson is that staff must work cooperatively with hospital security in such situations. Staff and physicians should be trained to alert security to such situations early, rather than waiting until the person becomes violent. By giving security a heads up, officers can move closer to the scene and respond more quickly when trouble

erupts, Dimoff says. They also can make themselves known to the person, which often discourages violence.

Homicide is relatively unusual in a health care setting, says **William Dunne**, MS, NREMT-P, director of the Office of Emergency Preparedness and administrative director of Security Services for the UCLA Health System in Los Angeles. Violence is not unusual, but it rarely goes so far as murder, he says.

"The statistics show an overall increase in violence in health care facilities in the past few years, but I also think there is an increased sensitivity to it also," Dunne says.

Dunne says the key to addressing violence in health care facilities is to create a culture of safety, rather than depending on more officers and more physical solutions, such as technology and infrastructure design.

"Those factors certainly can play a role, but it is more important to create a team in which people are always on the lookout for people who might act out or those who are acting suspiciously," he says. "That kind of culture will help you mitigate these situations, so that either they never become violent or you minimize the impact when it happens."

Shows limits of planning

The shootings show some of the limitations of preparations for violence in a health care setting, notes **Roberta Carroll**, ARM, CPCU, MBA, senior vice president, Aon Solutions, Chicago. There is every indication that Johns Hopkins was well prepared and had trained staff for violent situations, she says, but sometimes there is no way to prevent them.

Metal detectors, for instance, are an impractical solution for health care facilities, she says. They would have to be used at every entrance, and most hospitals have many. They also would have to be staffed around the clock by trained personnel.

"And besides, you don't want your hospital to look like an armed fortress," she says. "It is reasonable to expect hospitals to take precautions and do what they can to avoid violent situations, but unless you want to lock down your hospital like a prison, you can't completely eliminate the chance that someone is going to walk [in] with a gun."

Johns Hopkins alerted employees and students at the hospital and the university campus soon after the shooting, says **Earl Stoddard III**, PhD, MPH, public health program manager with the Center for Health & Homeland Security at the University of Maryland in Baltimore. He is a former Hopkins student and still on the school's e-mail list, so he received an e-mail about the incident within 10 minutes, he says. Hopkins also used the social networking site Twitter to send out alerts.

"Their flash messaging to both employees and students in the surrounding school buildings was quick," he says. "Their overall planning seemed to have worked well. Their emergency operations plan, which includes the scenario of an active shooter, was put into place quickly. They also worked well with the city police response."

An active shooter makes evacuation of an entire facility difficult or inadvisable, Stoddard says. An emergency plan should include provisions for notifying staff to stay and shelter in place, rather than risk leaving their workspaces and running into the shooter, Stoddard says.

"At Johns Hopkins, a nurse on the floor recognized immediately that something was wrong and got everyone out of the immediate area, then called security, which locked it down," he says. "That isolated the danger. In that regard, it appears their plan was very successful."

Conduct annual security evaluations

Stoddard advises hospitals to conduct security evaluations each year. A first step should be reviewing violent incidents from the previous year, along with near-violent incidents in which people feared someone would become violent. That information can reveal a great deal about the level of risk and the type of risk faced in your facility, he says.

"The risk is going to be different with every facility, but hospitals serve different populations, they have different stress loads, and nothing is ever the same. By looking at your own experiences, you can know how much attention to pay and how much of your resources to devote to this issue," he says. "Staff training and a constantly evolving security plan are key to managing these problems."

Stoddard points out that the training should include all employees of the facility, not just clinical staff. While clinical staff may be the most at risk, anyone working in the facility can become a victim if someone becomes violent, he says.

"Everyone should be expected to have an understanding of the emergency plan and security procedures," Stoddard says. "When an incident happens, it may not be a security person who responds and makes a difference in the first few

minutes. It might be a clinician or someone in accounting, so everyone needs to know the plan."

SOURCES

- **Sean Ahrens**, CPP, BSCP, CSC, Senior Security Consultant, Schirmer Engineering, Glenview, IL. Telephone: (847) 953-7761. E-mail: sean.ahrens@aon.com.
- **Roberta Carroll**, ARM, CPCU, MBA, Senior Vice President, Aon Solutions, Chicago. Telephone: (312) 381-1000.
- **Timothy Dimoff**, CPP, Founder and President, SACS Consulting and Investigative Services, Akron, OH. Telephone: (330) 2515-1101. Web site: www.sacsconsulting.com.
- **William Dunne**, MS, NREMT-P, Director, Office of Emergency Preparedness and Administrative Director, Security Services, UCLA Health System, Los Angeles. Telephone: (310) 206-3281. E-mail: rdunne@ mednet.ucla.edu.
- **Earl Stoddard III**, PhD, MPH, Public Health Program Manager, Center for Health & Homeland Security, University of Maryland, Baltimore, MD. Telephone: (240) 777-2323. E-mail: estoddard@law.umaryland.edu. ■

Personal touch might defuse potential violence

Focusing more on personal interactions can defuse potentially violent situations, says **Sean Ahrens**, CPP, BSCP, CSC, senior security consultant with Schirmer Engineering in Glenview, IL.

Ahrens previously worked in a hospital security position, and he encouraged staff there to use personal contact as a way to reduce the stress levels of patients and family members, which in turn lowered the risk of violence. Training in violence prevention should include urging staff and physicians to remember that others do not see their workplace the same way they do.

For those working at the hospital, it is a familiar place, and even the stress and unpleasant acts are something they experience all the time. For patients and family members, the hospital can appear quite different.

"When I come into the emergency department with my little girl who's cut her hand badly, this is the biggest thing in my life right now, and I'm going to be scared and anxious and very defensive about my little girl," he says. "Now to the triage nurse, this is just another day at work. It's good for the nurse to remain calm, of course, but you have to remember that the patient and the family are not at their best. They're scared, and they could be capable of violence if they felt like they're being ignored."

Increasing personal contact is a good way to reduce that stress, especially in the emergency department, he says. When people wait for long periods in the emergency waiting room, they become increasingly anxious and frustrated, and going back to the triage nurse and demanding treatment only makes matters worse.

One solution is to have staff members circulate through the emergency department frequently to make contact with those waiting. Ideally, both a nurse and a representative from patient services should circulate. The nurse can evaluate the patients for any change in their conditions and reassure them that they will be seen as soon as possible, and the patient services representative can offer practical aid and comfort.

"It can make a big difference if someone comes by and offers concern that you've been waiting and offers to get some crackers and juice for your kids," he says. "We had a patient services representative assigned to the emergency department all the time for just that reason. It doesn't look like a function of security and preventing violence, but in the end, that's what you might be doing." ■

ED violence vs. nurses remains high

Every week, in the United States, between 8% and 13% of emergency department nurses are victims of physical violence, according to a new study released by the Emergency Nurses Association (ENA) in Des Plaines, IL.

More than half the nurses (a mean of 54.8%) surveyed by ENA reported experiencing physical or verbal abuse at work in the last seven days. The Emergency Department Violence Surveillance Study also found that 15% of the nurses who reported experiencing physical violence said they sustained a physical injury as a result of the incident, and in almost half of the cases (44.9%), no action was taken against the perpetrator. ENA President **Diane Gurney**, RN, MS, CEN, says that result is particularly disturbing.

"We are extremely alarmed that there are so many cases in which hospitals do not respond to violence in the emergency department," Gurney says. "These incidents are not only frightening and dangerous for nurses, but also for patients in the emergency department. Hospital administration has a responsibility to keep patients and the health care providers who care for them safe. Every hospital

should be required to adopt and implement policies to keep their emergency departments safer."

Three in four nurses (74.4%) who were victims of physical violence reported that the hospital gave them no response regarding that violence. Nurses working in emergency departments at hospitals with policies regarding violence reported experiencing fewer incidents of physical or verbal violence. Hospitals with zero-tolerance reporting policies had an 8.4% physical violence rate; hospitals with a non-zero-tolerance policy had a 12.3% physical violence rate; and hospitals with no policy had an 18.1% physical violence rate.

The study revealed that certain physical safeguards are correlated with lower rates of violence. The presence of a panic button or silent alarm is associated with lower physical violence rates. Having an enclosed nurses' station, security signs and well-lit areas are associated with significantly lower verbal abuse rates.

Patients and their relatives were the perpetrators of the abuse in nearly all incidents of physical violence (97.1 %) and verbal abuse (91%). The majority of incidents of physical violence occurred in patients' rooms (80.6%). Nearly a quarter (23.2%) occurred in corridors, hallways, stairwells or elevators and only 14.7% occurred at the nurses' station. ■

CNE OBJECTIVES

Upon completion of this educational activity, participants should be able to:

- describe the legal, clinical, financial and managerial issues pertinent to risk management;
- explain the impact of risk management issues on patients, physicians, nurses, legal counsel and management;
- identify solutions to risk management problems in health care for hospital personnel to use in overcoming the challenges they encounter in daily practice. ■

COMING IN FUTURE MONTHS

■ Using metrics to improve your program

■ Lawsuits on the increase, report says

■ Language interpreters — how much is enough?

■ Appellate decision limits document demands

CNE 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 semester's activity with the **December** issue, you must complete the evaluation form provided and return it in the reply envelope provided in that issue in order to receive a certificate of completion. When your evaluation is received, a certificate will be mailed to you.

17. According to her lawsuit, what does Margaret O'Connor, RN, the former risk manager at Jordan Hospital in Plymouth, MA, allege was the reason for her firing?
A. She reported an EMTALA violation.
B. She reported a violation of anti-kickback laws.
C. She refused to self-report an EMTALA violation.
D. She approved a patient's transfer to another facility.

18. What is the monetary penalty for an EMTALA violation?
A. $25,000
B. $50,000
C. $75,000
D. $100,000

19. In the mammography fraud case at Perry Hospital, how was the fraud initially detected?
A. An internal quality check by the hospital
B. Reports from suspicious patients
C. A radiology group's query about missing mammograms
D. A criminal investigation

20. In the shooting at Johns Hopkins, what precipitated the violence, according to witnesses?
A. Patients fighting while waiting in the emergency department.
B. A physician discussing a patient's poor prognosis with her son.
C. A nurse refusing to provide medication to a patient.
D. A security officer discovering a theft in progress.

ANSWERS: 17. A; 18. B; 19. A; 20. B

United States Postal Service
Statement of Ownership, Management, and Circulation

1. Publication Title	2. Publication No.	3. Filing Date
Healthcare Risk Management	1 0 8 1 - 6 5 3 4	10/01/10
4. Issue Frequency	5. Number of Issues Published Annually	6. Annual Subscription Price
Monthly	12	$499.00

7. Complete Mailing Address of Known Office of Publication *(Not Printer) (Street, city, county, state, and ZIP+4)*
3525 Piedmont Road, Bldg. 6, Ste. 400, Atlanta,
Fulton County, GA 30305

Contact Person: Robin Salet
Telephone: 404/262-5489

8. Complete Mailing Address of Headquarters or General Business Office of Publisher *(Not Printer)*
3525 Piedmont Road, Bldg. 6, Ste. 400, Atlanta, GA 30305

9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor *(Do Not Leave Blank)*

Publisher *(Name and Complete Mailing Address)*
Robert Mate, President and CEO
AHC Media LLC, 3525 Piedmont Road, Bldg. 6, Ste. 400, Atlanta, GA 30305

Editor *(Name and Complete Mailing Address)*
Karen Young, same as above

Managing Editor *(Name and Complete Mailing Address)*
Russ Underwood, same as above

10. Owner *(Do not leave blank. If the publication is owned by a corporation, give the name and address of the corporation immediately followed by the names and addresses of all stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, give the names and addresses of the individual owners. If owned by a partnership or other unincorporated firm, give its name and address as well as those of each individual. If the publication is published by a nonprofit organization, give its name and address.)*

Full Name	Complete Mailing Address
AHC Media LLC	3525 Piedmont Road, Bldg. 6, Ste 400
	Atlanta, GA 30305

11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities. If none, check box → ☐ None

Full Name	Complete Mailing Address
Thompson Publishing Group Inc.	805 15th Street, NW, 3rd Floor
	Washington, D.C. 20005

12. Tax Status *(For completion by nonprofit organizations authorized to mail at nonprofit rates.) (Check one)*
The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes:
☐ Has Not Changed During Preceding 12 Months
☐ Has Changed During Preceding 12 Months *(Publisher must submit explanation of change with this statement)*

PS Form **3526**, September 1998 *See instructions on Reverse)*

13. Publication Name: Healthcare Risk Management
14. Issue Date for Circulation Data Below: September 2010

15. Extent and Nature of Circulation			Average No. of Copies Each Issue During Preceding 12 Months	Actual No. Copies of Single Issue Published Nearest to Filing Date
a. Total No. Copies *(Net Press Run)*			1056	1064
b. Paid and/or Requested Circulation	(1)	Paid/Requested Outside-County Mail Subscriptions Stated on Form 3541. *(Include advertiser's proof and exchange copies)*	671	716
	(2)	Paid In-County Subscriptions *(Include advertiser's proof and exchange copies)*	0	0
	(3)	Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Non-USPS Paid Distribution	50	53
	(4)	Other Classes Mailed Through the USPS	46	56
c. Total Paid and/or Requested Circulation *(Sum of 15b(1) and 15b(2)*			767	825
d. Free Distribution by Mail *(Samples, Complimentary and Other Free)*	(1)	Outside-County as Stated on Form 3541	15	15
	(2)	In-County as Stated on Form 3541	0	0
	(3)	Other Classes Mailed Through the USPS	0	0
e. Free Distribution Outside the Mail *(Carriers or Other Means)*			20	20
f. Total Free Distribution *(Sum of 15d and 15e)*			35	35
g. Total Distribution *(Sum of 15c and 15f)*			802	860
h. Copies Not Distributed			254	204
i. Total *(Sum of 15g. and h.*			1056	1064
Percent Paid and/or Requested Circulation *(15c divided by 15g times 100)*			96%	96%

16. Publication of Statement of Ownership
Publication required. Will be printed in the November 2010 issue of this publication. ☐ Publication not required.

17. Signature and Title of Editor, Publisher, Business Manager, or Owner: President and CEO — Date: 9/28/10

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including multiple damages and civil penalties).

Instructions to Publishers

1. Complete and file one copy of this form with your postmaster annually on or before October 1. Keep a copy of the completed form for your records.
2. In cases where the stockholder or security holder is a trustee, include in items 10 and 11 the name of the person or corporation for whom the trustee is acting. Also include the names and addresses of individuals who are stockholders who own or hold 1 percent or more of the total amount of bonds, mortgages, or other securities of the publishing corporation. In item 11, if none, check the box. Use blank sheets if more space is required.
3. Be sure to furnish all circulation information called for in item 15. Free circulation must be shown in items 15d, e, and f.
4. Item 15h., Copies not Distributed, must include (1) newsstand copies originally stated on Form 3541, and returned to the publisher, (2) estimated returns from news agents, and (3), copies for office use, leftovers, spoiled, and all other copies not distributed.
5. If the publication had Periodicals authorization as a general or requester publication, this Statement of Ownership, Management, and Circulation must be published; it must be printed in any issue in October or if the publication is not published during October, the first issue printed after October.
5. In item 16, indicate date of the issue in which this Statement of Ownership will be published.
6. Item 17 must be signed.

Failure to file or publish a statement of ownership may lead to suspension of second-class authorization.

HIPAA Regulatory Alert

Supplement to *Healthcare Risk Management* and *Hospital Access Management*

Don't wait: Start reviewing BA agreements now

Business associates a liable for breaches as covered entities

Although business associates are now subject to compliance with the HIPAA Security Rule and the use and disclosure provisions of the HIPAA Privacy Rule, as a result of the Health Information Technology for Economic and Clinical Health (HITECH) Act, hospitals should not assume business associates are taking steps to ensure their compliance.

"There is no requirement that covered entities [CEs] police their business associates and make sure they are compliant, but it is in the best interest of both organizations to make sure the business associates have everything in place," says **Robert W. Markette, Jr.**, an attorney with Gilliland & Markette in Indianapolis. "Within the business associate agreement, the CE is asking the business associate to affirm that programs are in place to comply with HIPAA requirements," he says. Most CEs, however, should take the extra step to double-check their key vendors to make sure everything is in place, he suggests. Once the rules are final, there will be a six-month window of time for business associates to finalize their programs to meet requirements; but six months is not a lot of time, he points out.

Business associate agreements should address the role and responsibilities of business associates in a privacy or security breach in more specific language. Address questions such as breach notification requirements and financial responsibility for responding to a breach, says **Phyllis A. Patrick**, MBA, FACHE, CHC, cofounder and managing director of AP Health Care Compliance Group, which has offices in Pittsburgh and Purchase, NY. "All that needs to be spelled out," she says.

In addition to making business associates subject to compliance with HIPAA requirements, a business associate's subcontractors must also be compliant, points out Patrick. "Business associates must also impose compliance requirements on their subcontractors, and a CE must include that requirement in their agreement with the business associate," she adds.

This is the time to start revising your business associate agreements, suggests Markette. "Although the rules are not final, I don't anticipate major changes from the proposed rules," he says. "Develop a new agreement form, but be prepared

EXECUTIVE SUMMARY

Hospitals should not make an assumption that business associates will automatically take all steps necessary to comply with the HIPAA Privacy Rule even though the Health Information Technology for Economic and Clinical Health (HITECH) Act mandates that they are subject to the same requirements as covered entities.

- Review business associate agreements to ensure language clearly specifies the business associate's role and responsibilities in a privacy or security breach.
- Refine your definition of business associate so that you can focus on vendors who do need access to protected health information in order to complete their work.
- Offer hospital resources such as training and forms to help the business associate comply with requirements.

Build a relationship with business associates

Strengthen HITECH compliance

One of the best ways to improve your relationship with business associates that handle protected health information (PHI) is to work with the vendor to ensure that the company has the resources to implement the proper staff training, documentation, investigative, or reporting procedures necessary to comply with HITECH, suggests Phyllis A. Patrick, MBA, FACHE, CHC, cofounder and managing director of AP Health Care Compliance Group, which has offices in Pittsburgh and Purchase, NY.

• Make sure business associates educate their employees about privacy and security requirements related to PHI.

"Hospitals have important resources that can be shared with business associates to educate their employees," says Patrick. Hospital representatives can visit the business associate, or representatives from the vendors or physician office staffs, can attend meetings related to HIPAA or HITECH, she suggests.

• Offer forms and documents related to HIPAA compliance to vendors to make sure they have the latest information.

"I have seen hospitals that set up vendor sections within their hospital website to communicate important information directly to vendors," says Patrick. "This same type of site can be used by vendors to download forms and updates."

• Designate one person as responsible and accountable for all activities related to business associates.

"Depending on the size of the hospital or covered entity, this might be the privacy and security officer or legal counsel," points out Patrick. "The most important factor in choosing someone to oversee business associate agreements is to make sure the person has the time to continuously monitor renewal of agreements as well as ongoing communications with vendors." ■

to modify it if necessary after the final rule is published," he adds.

Although you need to prepare a business associate agreement that complies with current requirements and anticipated requirements, you don't have to redo all vendors' contracts or agreements at once, says Patrick. "If you are at the point where a new contract is due, incorporate the up-to-date agreement," she says.

Another way to prepare for revision of all business associate agreements is to take a close look at who you have designated as a business associate, suggests Patrick. "I have heard people say that their hospital has 2,000 business associates," she says. "That is an unbelievably high number of business associates," she says. One reason for the high number could be an automatic assumption that all vendors must sign a business associate agreement to comply with HIPAA, she says. "If the vendor does not have access to protected health information [PHI] as part of their job with the hospital, there is no need to classify the vendor as a business associate for HIPAA purposes," she says.

Conduct a risk analysis for your vendors to identify which really accesses PHI, suggests Patrick. "The vendor who shreds your documents definitely should sign a business associate agreement, while the company that cleans your offices probably should not sign one," she says. "Even I've been asked to sign business associate agreements by clients for projects where I have not needed access to PHI to complete the work for the hospital," she points out. By evaluating who is a true business associate, you can cut down the number of agreements you need to track and modify, she adds.

Once you've identified your true business associates, develop a relationship with them that will improve communications during a potential breech, suggests Patrick. (See story above for tips on working with vendors.) "You may not be able to meet with all of your vendors during the year, but you should be able to hold periodic conversations with your high-risk vendors," she says. One way to identify key vendors is to involve department managers who work with different vendors, she says. "This helps prioritize vendors who have the most access to PHI, and it helps educate managers about HIPAA and HITECH regulations

and their part in ensuring compliance," she says.

Because CEs have up to 60 days to identify a potential breach, investigate it, and notify affected parties, it is critical that your business associates report their suspicions or discovery of a potential breach as soon as possible, says Markette. "I usually put 'within 24 hours' into the agreements," he says. The business associate may have investigated a potential breach and determined that no information was compromised, but the CE still needs to know, he points out. "If the business associate says there was a breach but the information was encrypted, it is reasonable for the CE to ask for proof that the information involved in the breach was encrypted."

[For more information about business associate agreements and HITECH requirements, contact:

***Phyllis A. Patrick**, MBA, FACHE, CHC, Co-Founder & Managing Director, AP Health Care Compliance Group. Phone: (914) 696-3622. E-mail: Phyllis@aphccompliance.com.*

***Robert W. Markette, Jr.**, Attorney, Gilliland & Markette, 3905 Vincennes Road, Suite 204, Indianapolis, IN 46268. Phone: (317) 704-2400 or (800) 894-1243. Fax: (317) 704-2410. E-mail: rmarkette@gillilandmarkette.com.]* ■

Access, not use, of PHI results in conviction

Doctor's conviction raises concerns for hospitals

Four months in prison and a $2,000 fine to Huping Zhou, a 47-year-old cardiothoracic surgeon from China and a UCLA health care system employee, for violating the Health Insurance Portability and Accountability Act (HIPAA) should be a cause for concern for hospitals.

"Prosecution and a prison sentence are significant in this case because there is no evidence that Zhou shared any of the protected health information [PHI] he accessed," says **Allyson Labban**, JD, senior associate in the Greensboro, NC, law office of Smith Moore Leatherwood. "The sentence sends a message to all health care employees that merely accessing information without a reason is a crime."

Zhou, a researcher at UCLA, reportedly began accessing and reading medical records of health care system employees, administrators, and celebrity patients following his notice of termination. In a three-week period, Zhou accessed more than 320 medical records for which he had no legitimate reason to access, says Labban.

"I do believe that hospital employees become complacent about following HIPAA requirements when there is no obvious breach of security or when private information is not shared outside the hospital," says Labban. In Zhou's case, UCLA cooperated with the Federal Bureau of Investigation and no charges were filed against the hospital, she points out. "Instead, prosecutors focused on the one individual." Although she does not know for sure, Labban believes that this indicates that the hospital had procedures in place to detect and report the breach.

Because it is obvious that attorneys general are willing to prosecute violators of HIPAA requirements, it is important for hospitals to take steps to limit access of records to employees who need access in order to perform their jobs, says Labban. "With the increasing use of electronic medical records, the ease with which employees can access records will only increase," she says.

Steps that hospitals should take now to prevent a similar situation include:

• Re-educate staff members about who can access records.

"Hospital staff members, especially physicians, are so accustomed to picking up charts and reviewing them that they don't think about whether or not it is appropriate," says Labban. Only physicians or hospital employees who are actively treating the patient or billing for that account, or supervising those activities should be accessing that record, she explains.

• Establish regular audits of medical records access.

"There is no set standard for how often an organization should audit access," says Labban. "Larger organizations may want to audit on a weekly or bi-weekly basis, while a smaller organization with fewer patients and charts might want to conduct an audit every month or two," she says. The key factors in determining how

often to audit are the number of records and the potential risk associated with inappropriate access to information.

• Review policies and procedures related to privacy and security of PHI.

"This is a good time to review policies in light of Zhou's conviction," says Labban. "Make sure policies clearly define who can access information and how to report inappropriate access."

[For more information about privacy and security requirements of HIPAA and HITECH, contact:

***Allyson Labban**, JD, Senior Associate, Smith Moore Leatherwood, 300 N. Greene Street, Suite 1400, Greensboro, NC 27401. Phone: (336) 378-5200. Fax: (336) 378-5400. E-mail: allyson.labban@smithmoorelaw.com.]* ■

Health care breach list tops 160

Insurance plans account for most records

Hospitals and provider networks lead the list of health care entities reporting breaches of unsecured protected health information (PHI), according to the Office for Civil Rights (OCR) breach notification website, which lists 166 entities as of Sept. 30.

Breaches that affect more than 500 individuals are included on the list, which includes the name of the entity, number of individuals affected, and date and type of breach as well as location of information that was breached.

According to a recent report by the Health Information Trust Alliance in Frisco, TX, hospitals and provider networks account for the greatest number of breaches, followed by physician practices. Insurance plans experienced the third highest number of breaches. However, due to the number of records at risk for each group, insurance plans' breaches affected the most individuals, with almost 3 million records breached.

To view the OCR breach website, go to www.hhs.gov/ocr, select "Health Information Privacy," then choose "HIPAA Administrative Simplification Statute and Rule" on the left navigation bar, select "Breach Notification Rule" on left bar, then choose "View Breaches Affecting 500 or More Individuals" on the bottom right corner of the page. ■

Looking at HIPAA security risks? Check your copier

Hard drives retain protected information

Time to upgrade some of your copiers? Are you planning to sell the old machines to recoup some money to use for new ones? Think twice before placing your "for sale" sign on the copier because you might be selling more than just the machine.

News reports from two different investigative news teams in different cities in the past year showed how easy it was to retrieve protected health information (PHI) from the hard drives in copy machines.

"A lot of copiers, and even fax machines, contain hard drives that store the information you copy or fax," points out *Jan Gibson*, JD, attorney with Baudino Law Group in Des Moines, IA. "One of the copiers in the news report came from a health insurance group and contained more than 300 medical documents for identifiable patients," she says.

Manufacturers are more aware of the need for privacy and security and have developed software that electronically shreds documents on a copier's hard drive, and there are machines that encrypt information, says Gibson. When a hospital is purchasing new copiers or fax machines that contain hard drives, the purchasing department should make sure they come with encryption and the ability to easily erase the hard drive, she recommends.

What about old machines? "Check with the vendor," suggests Gibson. "There may be a way to delete the data, or you may have to remove and destroy the hard drive," she says. Whichever route you choose, she adds, "don't just put the item up for sale. You might be selling a great deal of PHI without even knowing it."

[For more information about HIPAA privacy and security risks related to technology, contact:

Jan Gibson, JD, Attorney, Baudino Law Group, 2600 Grand Avenue, Suite 300, Des Moines, Iowa 50312. Phone: (515) 282.1010. Fax: (515) 282.1066. E-mail: Gibson@baudino.com.] ■

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

Nursing Home's Failure to Administer Laxative to Resident Leads to Death; $5.3M Verdict

by: **Radha V. Bachman, Esq.**
Buchanan Ingersoll & Rooney PC
Tampa, Florida

Lynn Rosenblatt, CRRN, LHRM
HealthSouth Sea Pines Rehabilitation Hospital
Melbourne, FL

News: A resident at an assisted living facility had significant issues with constipation and bowel issues for which she was prescribed certain medications. The resident claimed that the nursing facility did not administer the medication as required by her physician and that she began showing signs of an obstruction after one week of failing to have a bowel movement. Enemas and other treatments were administered by nurses at the facility, but ultimately she was taken to the emergency room with a ruptured colon. The woman died a few days later. A $5.3 million verdict was entered against the defendant in Tennessee.

Background: An 84-year-old woman was admitted to an assisted living facility in mostly good health. The woman's most significant problem was chronic constipation, for which she was prescribed certain laxatives. Over the course of a month, the woman typically received 60 doses of the medication. The woman complained that she was not being given adequate doses of the medication to control her constipation and bowel issues. The woman ultimately began showing signs of an obstruction, as she had not had a bowel movement in more than a week. The facility's nurses attempted to administer an enema and other treatments but were unsuccessful. The woman's abdomen became distended, and she worsened. She was rushed to the emergency room, where she was diagnosed with a ruptured colon. She passed away a few days later from sepsis caused by the rupture.

The plaintiff in this case alleged negligence due to the facility's failure to administer the laxative as required. During the two months prior to the woman's death, only 16 doses of the medication were administered in each of those months. The plaintiff also claimed that the facility's use of an enema in the face of an obstruction was also negligent. The defendant countered that the woman's condition worsened because the woman failed to discuss the issue with the facility's employees, and that the bowel rupture was not due to constipation, but attributable to a twisted colon. The defendant sought to compel arbitration based on documents signed by the woman. However, the court denied the motion, claiming that the defendant had waived its right to arbitration by actively participating in the discovery process.

The jury returned a verdict of $300,000 for compensatory damages and $5 million in punitive damages. Punitive damages were also assessed against the facility's two participating nurses. The verdict totaled $5,315,000.

What this case means to you: The background narrative indicates that the patient resided in an assisted living facility, which has a very different connotation from a skilled nursing and/or long-term care facility in terms of staffing and skilled services. Every state has very different licensure requirements for assisted living, as opposed to skilled nursing, which is generally regulated by Medicare. Long-term care in a nursing home is also state-regulated and highly specific.

Assisted living facilities can be anything from apartment residences with meals and housekeeping options to fully assisted care with the custodial activities of daily living. They can be large buildings that are corporately owned or private room-and-board residences. In many states, size dictates the need for licensure, and small private homes with four or fewer residences may be exempt from oversight, but still very much liable for neglect.

Generally, an ALF is not licensed to provide skilled nursing services, and the resident depends on private or Medicare-reimbursed home health services, as needed, based on medical presentation. In most ALF settings, the resident is responsible for providing his or her own medications, but may be given assistance with taking them — much as one would expect in a family-oriented situation, where an adult child provides oversight on the daily activities of a parent.

As a rule, larger ALF facilities employ licensed nurses to oversee residents, particularly in regard to daily medications. The resident takes the medications (both prescription and/or over the counter) with the nurse assuring that the resident actually takes them as prescribed, timely and accurately. Consistent with this approach is a daily assessment of the resident's personal presentation and/or any unusual behavior or adverse event that may indicate problems arising.

This elderly woman clearly suffered from professional neglect reflective of a diminished standard of care. In such non-skilled settings, nursing assessments may or may not include a full medical record, whereas in a skilled long-term care facility, one is always required. Nonetheless, that does not remove the obligation of appropriate oversight and reporting. Constipation and laxative dependence are exceedingly common in the elderly population, as is urinary retention and incontinency, so elimination patterns should be a prime consideration in the daily monitoring of residents in any setting.

Her history indicated that her primary problem was constipation and that she was laxative-dependent. The narrative indicates that she was aware that she had become constipated and complained that she felt she was not receiving sufficient doses of her regular laxative medication. Apparently, her concerns were disregarded. It appears that she was not being assessed for constipation, as she became obstructed. Bowel obstruction has obvious signs, and in a healthy adult almost always is the result of unresolved constipation. Increased-strength laxatives and enemas are safe and effective only in the early stages of impaction. Once the colon is obstructed, they can be very dangerous and can actually cause rupture. Emergency care was initiated — but far too late to prevent this unfortunate death.

There was no indication that an assessment of her elimination pattern was ever conducted upon admission or during her stay at the ALF. Therefore, the licensed staff that was overseeing her medications had no basis on which to assess any potential for problems, other than the concerns voiced by the resident, which may not be accurate or credible. This strongly suggests that some manner of assessment and report should exist in any setting where a proprietor assumes responsibility for the custodial care of a resident.

It does not appear that once the resident reported that she felt she was constipated that her bowel frequency was monitored to determine the severity of the problem. There are also indications that her laxatives were not administered as ordered, or that no one was aware that she required laxatives that frequently, which could be the case if she was dependent on non-prescription over-the-counter (OTC) medications. There was no indication that any type of record was being kept on the effects of the medications that were being administered. As many elderly patients frequently rely on OTC medications for the inconveniences of old age, a personal history upon admission is essential to safety and health management. A daily record of medications, including non-prescription drugs, that is updated on a regularly scheduled basis, such as a common MAR, is a standard practice of care where medication oversight is required. As many foods and commonly used OTC drugs have significant interactions with prescription medications, a medication administration record is essential.

Additionally, in an ALF, there should be a defined plan of care that delineates the resident's daily custodial care needs and an assessment of his or her overall condition that is passed off between shifts. This should be reviewed regularly at a team meeting together with the MAR and any information provided by family and from physician visits. All relevant information should be kept in the resident's health folder under HIPAA guidelines. Had all this been in place, this disaster would have been avoided.

REFERENCE

Bedford County (TN) Circuit Court, Case No. 10204. ■

Morphine overdose leads to brain injury

News: A woman underwent reconstructive breast surgery following breast cancer treatment. While in recovery, the woman suffered a morphine overdose that ultimately led to the woman suffering a brain injury. The plaintiff suffers significant lapses in judgment, memory, and executive function. A $1.67 million bench verdict was entered in favor of the plaintiff in Florida.

Background: Following breast cancer treatment, a woman underwent breast reconstructive surgery. During the surgery, the woman received 10 milligrams of morphine. She was prescribed 16 milligrams of morphine to be administered in 2 milligram shots upon arrival in the post-anesthesia care unit (PACU). The woman also was placed on a patient-controlled pump for morphine in the PACU from which she received 8 milligrams of morphine. Although the woman had used morphine and other opioid-based painkillers in connection with past surgeries, she was not considered "opioid tolerant." Opioid tolerance develops in patients who use a daily dose of opioid medication, or multiple doses per day, over a prolonged period of time, thereby conditioning their livers to break down the medication. By comparison, the woman's sporadic past use of morphine would not have allowed her to build a tolerance.

When the woman was transferred to a floor, she was not placed on telemetry for monitoring. Instead, a baby monitor was utilized to monitor for alarms from the PCA pump in the woman's room. The standard orders from the PACU, which were written by a physician earlier that day, were still in effect: The nurses were to assess and document the woman's level of arousal and respiration rate once per hour for four hours, and to notify a doctor if her systolic blood pressure dropped below 90, pulse rate below 60, or respiratory rate below 10. Under the hospital's "Nursing Service Clinical Alarms Policy," telemetry floor nurses were required to use baby intercoms for patients hooked up to PCA pumps. A registered nurse on the floor activated the baby intercom in the woman's room, so that telemetry staff would be notified immediately if the pump malfunctioned. Another floor nurse acknowledged that the baby intercom would pick up sounds from any other local alarm in the woman's room, such as the alarm from a pulse oximeter.

After about an hour of being on the floor, the woman's husband complained to the floor nurses that the woman was not breathing. An evaluation revealed that the woman was breathing one to two times per minute and that she had an oxygen saturation level of 75%. She was given supplemental oxygen, and physicians prescribed a drug used to counter the effects of opioid overdose.

Due to her injuries, the woman requires permanent medical care, therapy, and treatment. She will also require future attendant care, supervision, and assistance, because her brain injury makes her dangerous to herself and others, and also because she cannot properly care for herself due to significant lapses in judgment, memory, and executive function.

The woman sued the hospital and claimed that a portable pulse oximeter should have been utilized — and that had such a device been used it would have been audible to the staff without an intercom because of the room's proximity to the nurse's station. The defendant argued that the woman was not at high risk for respiratory depression from morphine and that her vital signs had been normal. The defendant further contended that the use of oximetry on the floor was not feasible. Had the woman needed constant monitoring, she would have been placed in the PACU or ICU. The experts agreed on several important points. They concurred that the woman had taken a significant amount of morphine and that respiratory depression is the main hazard of morphine use. They also agreed that each patient reacts differently to the drug, and it is difficult to predict who may suffer respiratory depression as a side effect. Both acknowledged various factors that can increase a patient's risk for respiratory depression, including age, morphine tolerance, the cumulative effect of morphine doses over a short period of time, and whether a patient gets drowsy or falls asleep while on the drug. Both agreed that the woman did not have a tolerance to opioids, and both seemed to accept the reality that she would be apt to fall asleep after a day of surgery. Finally, both acknowledged that the hospital's health care workers have a duty to observe patients as required by the relevant standard of care, regardless of what may be indicated on doctor's orders or by hospital policies.

The matter went to a bench trial and the court awarded a total of $1.6 million.

What this case means to you: This is an unfortunate outcome to a procedure that has become routine and in reality was not the issue in the woman's anoxic brain injury. One can only assume that the surgery went as expected, and had it not been for the lapse in the post-operative care that the patient received, she would have survived and lived out her life as she and her husband fully expected her to do.

There is no discussion as to the type of anesthesia that the patient received, any effect that it may have had on her pain, or how it was to be managed post-operatively. Generally, morphine has a cumulative effect, particularly in the presence of other central nervous system depressions. The morphine administered during the procedure was to be supplemented by an additional 16 milligrams of morphine in 2 milligram doses while in the PACU, but the narrative does not provide a time frame for completion of the eight separate doses. Since there was also an order for a patient-controlled pump, there is always the possibility that the initial order for the 16 milligrams in equally divided doses was the formula for the PCA, of which she received 8 milligrams of the original 16 milligram dose. If the patient actually got the initial 10 milligrams in surgery plus an additional 16 milligrams and then 8 milligrams more over her stay in the unit, she most likely was at risk for respiratory depression.

Whatever the order, the patient's past use of morphine and the possibility of tolerance needed to be substantiated rather than assumed. Pain management in a post-surgical setting is always based on patient monitoring and response. The PACU nurse receiving the patient from the surgical suite should have verified and documented the patient's vital signs on arrival and at pre-established intervals over her stay in the unit. Electronic monitoring in such units is a standard of care, so the assumption is that when she was transferred to the floor her vital signs were stable. It can also be assumed that her pain was suitably managed and that a full report was provided between the PACU nurse and the nurse who was to assume responsibility for the patient on the floor.

Once on the floor, the nurse there would have taken a full report from the PACU and assessed the patient for post-surgical stability to include vital signs and break through pain. Generally when a patient is transferred to another unit, standard policy is to reassess the patient every 15-20 minutes, 1-2 hours, and then at diminishing frequency, based on the patient's condition and stability.

In this case, the physician ordered the assessment to be done every hour with parameters for four hours. Obviously, since she was in crisis within an hour, this was not adequate to detect respiratory compromise. The nurse had responsibility to assure the patient's ongoing stability, and knowing that she had already received at least 18 milligrams of morphine, in addition to anesthesia and any other pre/post-operative medications, the assessments initially should have been more frequent.

From the narrative, it appears that hospital policy dictated telemetry floor nurses use "baby monitors" for patients on PCA pumps. There is a disconnect here, as was there an assumption by the physician that the patient would be on telemetry and be actively monitored — or was the assumption by the floor nurse that because a "baby monitor" was in use that the telemetry nurses would assume responsibility for monitoring the PCA alarm? Since the patient was not assigned to telemetry, it would not appear that the telemetry nurses had any responsibility to monitor the alarms, and the "baby monitor" was not an appropriate substitute to pulse oximetry or some other electronic surveillance device.

The floor nurses violated the accepted standard of care, which is to frequently monitor a patient who has received high doses of a central nervous system depressant for respiratory compromise. They apparently assumed that responsibility fell to the telemetry staff, who in reality had no responsibility for this patient. Why she was not assigned to the telemetry unit remains unclear, but that may have made a difference in the outcome. The patient arrested and sustained an anoxic brain injury because of this mismanagement of what should have been a routine case.

The experts agreed on several key points that clearly established liability on the part of the hospital in respect to the standard of care provided by the floor nurses. At this point, it may have been prudent for the hospital to have entered into some sort of mediation that would have spared a trial and given more control in terms of settlement to the hospital. On the other hand given the woman's impairments from her brain injury, the $1.6 million over her lifetime may well have been a reasonable financial settlement for both sides.

REFERENCE

U.S. District Court, Southern District of Florida, Case No. 09-23360. ■