HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE FOR MORE THAN THREE DECADES

INSIDE

AHC Media

MARCH 2015 Vol. 37, No. 3; p. 25-36

Nurse fatigue a 'huge' threat to patient safety, but can be addressed

When fatigue is addressed in the healthcare workplace, attention often goes first to physicians and particularly medical residents who are sleep-deprived and overworked. Increasingly, risk managers are focusing on the patient safety threats posed by nurses and other staff members who are too tired to do their jobs properly.

Fatigue poses a "huge" threat to patient safety, says **Richard C. Boothman**, JD, chief risk officer and executive director of clinical safety at the University of Michigan Health System in Ann Arbor. The healthcare industry has not connected the dots between how clinical and business pressures can fatigue nurses to the point of threatening patient safety, he says.

> ... THERE IS A 3.4% CHANCE OF AN ERROR OCCURRING WHEN NURSES OBTAIN SIX HOURS OR LESS OF SLEEP DURING A 24-HOUR PERIOD.

"Fatigue is a pretty well documented concern, but it is not often related to nurses," Boothman says. "We went through years of worry about resident work-hour restrictions, and we keep meticulous records of how many hours residents work, and truck drivers are under some stringent restrictions. There is no reason to think nurses are immune to the same problem, and in some ways it's worse."

The problem can be worse because nurses have the most direct contact with patients, and fatigue-induced errors or oversights can start a chain reaction of improper care, Boothman explains. Nurses also can be more susceptible to fatigue than residents because the nurse is working constantly through the shift, unlike residents who work long hours but can rest when they have time, he says.

Financial Disclosure: Author Greg Freeman, Executive Editor Joy Daughtery 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.

HEALTHCARE RISK MANAGEMENT™

Healthcare Risk Management™,
ISSN 1081-6534, including HRM Legal Review & Commentary™ is published monthly by
AHC Media, LLC
One Atlanta Plaza
950 East Paces Ferry Road NE, Suite 2850
Atlanta, GA 30326.

Periodicals Postage Paid at Atlanta, GA 30304 and at additional mailing offices.
GST Registration Number: R128870672.

POSTMASTER: Send address changes to:
Healthcare Risk Management
P.O. Box 550669
Atlanta, GA 30355.

SUBSCRIBER INFORMATION:
Customer Service: (800) 688-2421.
customerservice@ahcmedia.com.
www.ahcmedia.com

SUBSCRIPTION PRICES:
U.S.A., Print: 1 year (12 issues) with free CE nursing contact hours, $519. Add $19.99 for shipping & handling. Online only, single user: 1 year with free CE nursing contact hours, $469. Outside U.S., add $30 per year, total prepaid in U.S. funds.

MULTIPLE COPIES: 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.) Missing issues will be fulfilled by customer service free of charge when contacted within one month of the missing issue's date.

ACCREDITATION: 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.

EXECUTIVE EDITOR: Joy Daughtery Dickinson (404) 262-5410 (joy.dickinson@ahcmedia.com).
DIRECTOR OF CONTINUING EDUCATION AND EDITORIAL: Lee Landenberger.

EDITORIAL QUESTIONS
Questions or comments?
Call Editor **Greg Freeman**, (770) 998-8455.

Boothman cites the infamous case of a highly regarded obstetrics nurse at St. Mary's Hospital in Madison, WI. In 2007, she worked her regular eight-hour shift on July 4 and volunteered to work an extra shift that same day. Scheduled for a 7 a.m. shift on July 5, she slept at the hospital at the end of the two shifts. During the second half of that July 5 shift, the nurse mistakenly gave intravenous bupivacaine (Marcaine, Sensorcaine) to a 16-year-old scheduled for induction of labor. The anesthetic, intended for epidural administration, had not been ordered. She was supposed to have given intravenous penicillin that had been prescribed to treat a streptococcal infection. The woman died from cardiac arrest, but her baby lived.

The nurse was charged initially with a felony, "criminal neglect of a patient causing great bodily harm," but was allowed to plead no contest to two misdemeanors. The Wisconsin Board of Nursing suspended her license for nine months, and she lost her job.

"Most of us in the business thought that treatment was incredibly unfair," Boothman says. "The hospital dangled financial incentives for her to work back-to-back or really long shifts."

The hospital determined that fatigue was one cause of the error, and it implemented a policy to limit hours worked. It also took several steps to improve the safety of medication administration, St. Mary's reports. *(For more on the incident and the hospital's response, see the story "Shaping systems for better behavioral choices: Lessons learned from a fatal medication error,"* Joint Commission Journal on Patient Safety and Quality, *April 2010, p. 152.*)

Comparable to alcohol

Risk managers must convince hospital leaders to see nurse fatigue as a patient safety risk, rather than a budgetary or human resources problem, Boothman says. Staffing ratios and scheduling should always factor patient safety into the decision-making process, he says.

"We've had blinders on about this for a long time," Boothman says. "Ironically, part of the problem is brought on by the caregivers, because they seem so dedicated that they often put their own health and concerns off to the side."

Naturally, the problem is more common and more serious in those settings that provide patient care 24 hours per day or those that require mandatory overtime, says **Robin Diamond**, MSN, JD, RN, senior vice president of patient safety and risk management at The Doctors Company, a malpractice insurer

EXECUTIVE SUMMARY

Nurse and staff member fatigue increasingly is recognized as a significant threat to patient safety. Risk managers should adopt strategies to reduce fatigue caused by scheduling, overtime, and excessive workloads.

- High turnover rates among nurses can indicate fatigue risks.
- Hospital culture must encourage staff to admit fatigue and to report fatigue in others.
- Creative scheduling can reduce nurse fatigue.

based in Napa, CA. But any setting is affected if staff are fatigued, whether it's by work schedules or a new baby at home, she says. The risk comes from attention lapses, inability to focus, slow reaction time, and confusion.

"Objective recordings by polysomnographic recorders verify that nurses, air traffic controllers, and even commercial truck drivers regularly fall asleep during night shifts," Diamond says. "Research has shown a significant relationship between sleep in the prior 24 hours and the risk of making an error. Some studies are comparing impairment to blood alcohol content, suggesting that a nurse awake for 19 hours is the same as having a blood alcohol content of 0.05%."

According to a study by Australian researchers, there is a 3.4% chance of an error occurring when nurses obtain six hours or less of sleep during a 24-hour period. This number might sound small, but **Bette McNee**, health and human services technical specialist with The Graham Company, a healthcare consulting firm in Philadelphia, PA, makes this point: If an average teaching hospital has 1,000 nursing shifts per day, this error percentage equals 34 daily errors. Over a year, that's more than 12,000 patients whose care is at risk because nurses aren't getting adequate sleep. *(An abstract of the study is available online at http://www.ncbi.nlm.nih.gov/pubmed/16099184.)*

"The most important thing a hospital can do is to create a culture that allows a nurse to say that he or she is tired and needs to take a short nap or a walk outside — a culture where the nurse doesn't worry about reprimand or disciplinary action for recognizing their own limitations," McNee says.

A punitive atmosphere will drive fatigue issues underground, says **Brandi Crow**, BSN, RN, who worked until recently as associate chief nursing officer at a major hospital and is now clinical analyst with MD Buyline, a company based in Dallas that provides information to make technology decisions. She recalls incidents in which a nurse and a physician were routinely too fatigued to provide safe care.

"We found that coworkers, everyone around these two individuals in their department, were really hesitant to report or confront the behavior," she says. "We knew right then that we were going to develop more trust about reporting. Every risk manager knows that the amount of good you can do depends on how much people are willing to report issues."

One strategy Crow used was to encourage nurses to buddy up during their shifts so they could watch each other for signs of fatigue and suggest a remedy. Pairing up makes them accountable to each other, she notes.

Rick managers must lead

Diamond says risk managers should assess the organization for fatigue-related risks such as understaffing, consecutive shift work, and policies that encourage overtime. A fatigue management plan should include education of staff about the effects of fatigue and good sleep hygiene, as well as making it a responsibility for staff members to intervene when they notice a colleague suffering from effects of fatigue.

Research has demonstrated that specific strategies work to revive a fatigued employee, Diamond says. The other person should engage the fatigued employee in active conversations, lead him or her into physical activity, and encourage strategic caffeine intake. Caffeine typically takes about half an hour to kick in, so a cup of coffee might be best before a nap, not after. The hospital also should provide areas for nurses to nap, with ear plugs and eye masks, just as many facilities do for physicians, Diamond says. *(See the story on p. 28 for more advice on addressing fatigue in the workplace. See the story on p. 29 for how refrigerator alarms contribute to fatigue.)*

"It also is important to provide opportunities for staff to express concern about fatigue," Diamond says. "Collect data on work hours, scheduling, absenteeism, workers' comp, job satisfaction, and adverse events. Always analyze fatigue when evaluating adverse events."

Boothman notes that the turnover rate can be a measure of how much fatigue is threatening patient safety. More than income, nurses tend to choose employment based on quality of life and satisfaction that they are helping their patients, he says. "Where people are asked to do too much with too little, you will see nurses moving in droves to other organizations," he says. "That can be a major red flag, so the risk manager should always keep a finger on the pulse of the hospital's nurse turnover rate. It's the best indicator of how happy your nurses are, and fatigue has a big effect on job satisfaction." *(See the story on p. 28 for information on how fatigue also can be a compliance issue.)*

Creative scheduling can greatly reduce nurse fatigue, says **Lydia L. Forsythe**, PhD, MA, MSN, RN, CNOR, an adjunct faculty member for the master of science in nursing (MSN) and doctor of nursing practice (DNP) programs at Kaplan University School of Nursing in Oklahoma City. Options include providing four-hour shifts,

providing two-hour bonus shifts, and prohibiting 12-hour shifts or any back-to-back shifts.

"Hospitals get stuck in the traditional way of thinking about scheduling, and it takes a really tenacious person to advocate for something that might sound radical but actually works out better for both nurses and patients," Forsythe says. "We also have to plan for the predictable spikes in patient population, like flu season. If you don't schedule for that, you end up needing people to work overtime and more shifts."

SOURCES

Richard C. Boothman, JD, Chief Risk Officer, Executive Director of Clinical Safety, University of Michigan Health System, Ann Arbor. Email: boothman@med.umich.edu.

Brandi Crow, BSN, RN, Clinical Analyst, MD Buyline, Dallas. Email: brandi.crow@mdbuyline.com.

Robin Diamond, MSN, JD, RN, Senior Vice President, Patient Safety and Risk Management, The Doctors Company, Napa, CA. Telephone: (707) 226-0291. Email: rdiamond@thedoctors.com.

Lydia L. Forsythe, PhD, MA, MSN, RN, CNOR, Adjunct Faculty Member, Kaplan University School of Nursing, Oklahoma City. Email: londes@cs.com.

Bette McNee, Health and Human Services Technical Specialist, The Graham Company, Philadelphia, PA. Email: BMcNee@grahamco.com. ■

Staff fatigue can be a compliance risk, too

Many healthcare leaders don't realize that, in addition to threatening patient safety, nurse fatigue is also a compliance risk, notes CEO **Nick Merkin** of Compliagent, a compliance consulting firm in Los Angeles.

In many states, certain healthcare facilities are required to maintain minimum staffing levels as a ratio of nursing hours per patient day, or other metrics, as a matter of state regulation, Merkin explains. The necessary calculations for making this determination are not so easy, however, as they might fluctuate depending on the acuity level of the patients under medical care that day, the skillset of the nurses on the floor at any given time, and many other variables. It takes real expertise to take all the relevant factors into consideration, give them appropriate weight, and have the right nursing resources in place and ready to deploy on short notice, Merkin says.

"The issue of fatigue is often brought up as a complaint from the nursing staff. Much of the concern seems to come from a perception from the nurses that their healthcare facilities are understaffed, shifts are too long, or that the rest periods during shifts are too brief," he says. "And as a result of the current financial stresses within the healthcare industry, the problem will only become more acute as providers are under more and more pressure to cut staffing costs."

Hitting the right balance with staffing and scheduling can be a challenge. The consequences of making the wrong call in this context can be severe, Merkin notes. On one hand, overstaffing is obviously expensive and is going to cut deeply into a healthcare provider's bottom line. On the other hand, understaffing can result in government enforcement actions carrying fines, penalties, malpractice suits, and class actions against healthcare facilities and managers.

"There are plaintiffs lawyers out there who literally are making a career out of identifying areas of alleged nursing fatigue caused by understaffing and leading to poor patient outcomes," Merkin says. "Healthcare providers who are not prepared from a compliance perspective are facing serious regulatory and financial risk."

SOURCE

Nick Merkin, CEO, Compliagent, Los Angeles. Email: nmerkin@compliagent.com. ■

Eight tips for addressing nurse fatigue

These tips for combatting nurse fatigue come from **Bette McNee**, health and human services technical specialist with The Graham Company, a healthcare consulting firm in Philadelphia, PA:

• **Consider not having 12-hour shifts.** Try 12-hour days with two six-hour shifts through the night to break up the work, or at least schedule the 12-hour shift in the daytime.

• **Consider your timing.** Don't have staff meetings at 7:30 a.m. Don't schedule meetings or parties after long shifts, forcing your staff to stay awake longer than they should.

• **Create staffing thresholds.** Allow no more than two consecutive 12-hour shifts and no more than four or five days straight without a day off. Weekly overtime hours should be allowed sparingly.

• **Consider four-hour block**

staffing. Pool and per diem staff might be more amenable to multiple four-hour shifts instead of fewer eight-hour shifts. Similarly, staff members might prefer taking two four-hour holiday breaks rather than one day off.

• **Share health promotion and wellness education materials.** Nurses, and particularly nurse managers, can't correct fatigue-inducing habits if they don't realize the connection. Provide your nurses with materials that help them learn and implement good sleep and holiday stress practices.

• **Create rest spots.** This rest spot doesn't have to be a room complete with beds and pillows. You can make a difference by providing a quiet, comfortable area where nursing staff members can take a 15- or 20-minute power nap to recharge mental alertness for the remainder of their shifts.

• **Serve free coffee.** The traditional pick-me-up does work to improve alertness, so free coffee is a small way to make a significant improvement.

• **Encourage exercise.** A few minutes on a treadmill or exercise bike can increase alertness and attention. ■

Refrigerator alarms can wear on staff

Medical device alarms aren't the only technology contributing to fatigue among nurses. Refrigerator alarms contribute to physical fatigue and alarm fatigue, says **Brian Balboni**, CEO of Primex Wireless, a company in Lake Geneva, WI, that provides wireless monitoring technology.

The Joint Commission requires hospitals to monitor and log the temperature of refrigerators used to store everything from medications and IV solutions to nutritionals, such as juices, Balboni notes. If the hospital is using standard data loggers, someone (almost always a nurse) must check the temperature on each data logger a minimum of twice a day and enter the reading on a log sheet.

"That means a nurse who already may not even have five minutes to grab a bite to eat must leave his or her patients to take on this additional task," Balboni says.

In addition, someone — again, usually a nurse — periodically will have to download the data from the data logger somehow to get the reports that the hospital needs to submit to The Joint Commission. "Where it really gets crazy is if a temperature reading goes out of range between visits, it will normally set off a local alarm," Balboni says. "That alarm's only purpose is to tell the nurse to contact maintenance immediately — yet another task that isn't exactly working at the top of a nurse's license."

A monitoring system that eliminates the need for manual logging and alarms can be a better solution, he says. The system will log the data electronically as well as send an automatic email, text, or phone alert directly to the person who is responsible for fixing the situation if a refrigerator goes out of range.

This method removes the need for the local alarm, helping reduce alarm fatigue and the risk of spoilage while eliminating additional, non-clinical work for nurses. Direct, alarm-free notification also can contribute to higher Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) patient satisfaction scores around Question 9 regarding how often the area around the room was quiet at night, Balboni notes. ■

Workers' comp claims expected to decrease in 2015

There's good news if the cost of workers' comp claims has been a problem at your hospital. The latest outlook calls for claims to decrease this year, which continues a trend over the past decade.

The second Health Care Workers Compensation Barometer report from Aon Risk Solutions in Atlanta explores trends in frequency, severity, and overall loss rates related to workers' compensation for about 1,150 U.S. healthcare facilities. The 2014 report projects workers' compensation loss rates will continue to decrease 1% annually.

The report also shows frequency of workers' compensation claims has been slowly and consistently decreasing over the past decade at the same 1% level, while claim severity has been slowly increasing at a rate of 2% per year, says **Martha Bronson**, ASA, MAAA, associate director and actuary in Aon Risk Solutions' Global Risk Consulting practice in Radnor, PA.

The report also analyzes survey data highlighting the specific concerns and issues that the healthcare industry faces. Patient management, including handling and lifting, has been identified as the number one concern by risk managers as it accounts for one-third of all claims and has the highest average indemnity payment

out of all causes of loss.

Patient handling is still the biggest concern for risk managers when it comes to workers' comp claims, Bronson says.

"Across the board, frequency is going down, and that's a positive for risk managers," Bronson says. "Severity is either holding steady or rising slightly in some states, but I think that's mainly because of inflation, the cost of care going up."

The decline in frequency might be attributed to a better awareness that patient handling is a risk to employees, Bronson says. More hospitals are making use of safety committees and utilizing lifting devices and other strategies for reducing the risk from patient handling, she says.

Other noteworthy key findings from Aon's report include:

• Ninety percent of survey respondents have a return-to-work program, but only 65% have metrics in place to test the effectiveness of the program.

• Ninety-five percent of survey respondents have a formal safety committee.

• Seventeen percent of survey respondents have a safety incentive program in place.

EXECUTIVE SUMMARY

New information on workers' compensation claims in healthcare predicts that claims will drop in 2015. Most hospitals have a return-to-work program but don't measure its effectiveness.

- The drop continues a trend from the past 10 years.
- Most hospitals don't have a safety incentive program.
- Sixty percent of nurses worry that their job is negatively affecting their health.

• For the 2015 accident year, Aon projects that healthcare facilities will experience an annual loss rate of $0.75 per $100 of payroll. This projection applies at the country-wide level and is made assuming a $500,000 per occurrence limit.

• Among the 11 states profiled within the report, California has the highest projected loss rate for 2015 at $2.18. Tennessee has the lowest projected loss rate for 2015 at $0.48.

• Home healthcare aides have the highest average indemnity cost among healthcare-related workers' compensation claims.

In addition to survey data, the 2014 report examines other workers' compensation trends in the healthcare industry, including claim frequency and severity by department and occupation. For the first time, the report analyzes the department and occupation fields within claim data to measure the relative frequency and severity of claims by department and occupation, separately.

The report also examines historical trends by state, providing statistical information on historical frequency, severity, and overall loss rates specific to 11 states: California, Florida, Kentucky, Maryland, Missouri, New Jersey, New York, Pennsylvania, South Carolina, Tennessee, and Virginia. *(The full report is available online at http://bit.ly/1CeyS2N. You must provide contact information to gain access.)*

SOURCES

Martha Bronson, ASA, MAAA, Associate Director and Actuary, Aon Risk Solutions, Global Risk Consulting Practice, Radnor, PA. Telephone: (615) 881-2679. Email: Martha.bronson@aon.com. ■

Injuries are a constant worry for nurses

Sixty percent of nurses worry that their job is negatively impacting their overall health, and one in 10 nurses were injured on the job in the past year. The report from Ergotron Healthcare, a company in St. Paul, MN, that sells ergonomic equipment to support digital activities in healthcare, also suggests that nurses' performance is harmed by physical discomfort.

The report, *How Digital Healthcare Helps and Hurts Nurses*, notes that when asked about the effects of injuries or discomfort, 22% of nurse respondents said they are less friendly or engaging with their patients. Another 22% said they have to modify or limit their activity or movement on the job. Seventeen percent said they are distracted, and 14% said they needed more assistance from other staff members. Twenty-five percent did not cite specific effects.

Nurse injuries have been well documented, but what is often not addressed is how their injuries and physical discomfort directly affects patient care, says **Steve Reinecke**, MT (CLS), CPHIMS, assistant vice president at Ergotron Healthcare.

When asked what they would change in their work environment to support the prevention of discomfort, pain, or injury to themselves and fellow nurses, 54% of the nurses in the Ergotron survey said they would increase nursing staff to alleviate

workloads, 28% would instate a dedicated ergonomics team to help ensure equipment is ergonomically supportive to the staff, and 28% would redesign the physical space within patient rooms and on floors to better align with clinical workflow and patient needs. In addition, 25% would update the furniture at the nursing station, 24% would update medical equipment and furniture in the patient room, and 22% would implement more point-of-care solutions throughout the floor. Respondents could choose more than one answer.

Ill effects from injuries and discomfort in the workplace can fly under the radar until they turn into a costly workers' comp claim, warns **Joe Paduda**, principal of Health Strategy Associates, a consulting firm in Madison, CT, specializing in managed care for workers' compensation and group health. Individual claims also can seem routine and relatively inexpensive, but if not managed well, they can turn into a significant liability.

"If anything points out the challenge faced by risk managers — with frequency declining and severity seemingly under control — it's how to get senior management's attention when it appears things are going along quite nicely," Paduda says. "The key is to identify those creeping catastrophics, the claims that seem to move along nicely, before veering off into the never-never land of opioids, permanent disability, and no resolution in sight. These are the anecdotal examples likely to generate a visceral response on the part of CFOs, a response that will provide the impetus needed to better manage these risks."

SOURCES

Joe Paduda, Principal, Health Strategy Associates, Madison, CT. Email: jpaduda@healthstrategyassoc.com.

Steve Reinecke, MT (CLS), CPHIMS, Assistant Vice President, Ergotron Healthcare, St. Paul, MN. Email: sreinecke@ergotron.com. ■

Infusion pumps are weak link in data security

Cyber security experts and healthcare leaders are warning that the biggest threat to your hospital system's data security might be one of the most innocuous, seemingly harmless devices that doesn't even appear to have anything to do with your computer system: the infusion pump.

The simple infusion pump poses a grave threat to system security, says **Linda Zdon**, director of information security and compliance at Allina, a 12-hospital health system based in Minneapolis. Allina spotted the issue during implementation of new infusion pumps recently, when engineers realized the pumps had little security but were connected to the rest of the hospital's computer system.

"Our network engineers raised some concerns to our security engineers that there could be a weakness with the infusion pumps," Zdon says. "Infusion pumps are much smarter than they used to be. Five or 10 years ago they were barely computerized, but now they are mini-computers connected by a wireless network so that data can be pushed to them and data can be harvested from them."

Infusion pumps are ubiquitous because almost every hospital patient uses them at some point, Zdon says. Allina has at least 3,000 across the system, she says. Allina has been working with the National Institute of Standards and Technology (NIST) in Gaithersburg, MD, to develop a "use case," which is a form of technical analysis, for wireless pumps. The goal is to develop new standards to harden medical devices against cyberattacks and computer viruses.

The American Hospital Association sent a letter to the Food and Drug Administration in November 2014 urging the federal government to hold device manufacturers accountable for cybersecurity. In December, NIST warned healthcare providers of the cyber risks from infusion pumps and noted that "[w]hile this technology has created more powerful tools and improved health care, it has led to additional risks in safety and security." *(See the story on p. 32 for more on the NIST warning.)*

The digitation of medical records and value of personal health information (PHI) on the black

EXECUTIVE SUMMARY

Infusion pumps pose a major risk to data security in healthcare facilities. The wireless connection to the pump often can be used to access the computer system.

- The pumps are much more computerized than in the past.
- Infusion pumps from the same vendor have the same login and password.
- Risk managers should demand improvements from vendors.

market makes the healthcare industry particularly vulnerable to data breaches, notes **Michael Bruemmer**, vice president of Experian Data Breach Resolution in Austin, TX. In fact, the healthcare sector represented about 42% of all major data breaches in 2014 alone, he says. He expects to see that percentage grow.

"In order to protect patient data and avoid hefty regulator fines, the industry needs to come up with a stronger solution to improve its cybersecurity strategies and be prepared for the likelihood of a data breach," Bruemmer says. "This means conducting frequent security training with employees, investing in the most up-to-date security technologies, and having a strong data breach response plan in place so a company can react immediately when a breach is discovered." *(For more on cyber security and response to a data breach, see* Healthcare Risk Management*, August 2014, pp. 78-81.)*

Addressing the risk can be challenging because vendors are more focused on the pump itself and offer little help with securing the network that the pump is connected to, Zdon says. Risk managers will have to work with their own network engineers to secure the network, with some input from the vendor, she says.

One difficulty is that infusion pumps from the same company have a single password for every pump across the country, Zdon says. That universal password makes it difficult to secure the unit itself from hackers, which practically eliminates the first step that any network engineer would want to take, she explains. But it also would not be practical for even every infusion pump in a facility to have its own unique password.

"We need to work with vendors to make the security of the individual devices better, but on the other hand if they make the security really good, at some point the device becomes almost unusable," Zdon explains. "It's a balancing act."

In the past, the IT department at healthcare facilities has not been responsible for managing infusion pumps because they were not computerized in a significant way, Zdon notes. Medical device managers or bioengineers were more likely to be responsible. Now, Zdon says, the risk manager might need to get both departments together to develop a security plan for infusion pumps.

Infusion pumps are a good example of companies trading easy access for security, says **Sergio Galindo**, president of GFI Software in Durham, NC, and a former hacker himself. He notes how often major software companies such as Microsoft and Adobe issue security fixes for their products, but infusion pumps have a similar underlying operating system that is rarely, if ever, updated. "Even if the infusion pumps need only a tenth of the security patches that Microsoft issues, there still should be significant updates that could respond to bugs or new developments in what hackers are doing," he says. "Hospitals need to put pressure on the vendors to treat these devices like the computers they are and not let them get away with saying they're just infusion pumps and not computers."

Before signing contracts with an infusion pump vendor, the hospital should require an explanation of how the vendor will issue updates, who they will go to at the hospital, and how the hospital's engineers can receive help from the vendor to secure the infusion pump network, Galindo says.

"One good strategy is to bring in an IT tester, sometimes called a 'white hat,' and have them go around the hospital to see what they can access," Galindo suggests. "Whether its infusion pumps, Wi-Fi, or a device that is broadcasting information that it shouldn't, a person with the same skills as a hacker can find your weak points."

SOURCES

Michael Bruemmer, Vice President, Experian Data Breach Resolution, Austin, TX. Email: bruemmer@experian.com.

Sergio Galindo, President of GFI Software in Durham, NC. Telephone: (781) 418-2474.

Linda Zdon, Director of Information Security and Compliance, Allina, Minneapolis. Email: linda.zdon@allina.com. ■

NIST explains why infusion pumps are weak link

The National Institute of Standards and Technology (NIST) in Gaithersburg, MD, recently issued a report on the security risk from infusion pumps. These are some excerpts from the report:

• Today, infusion pumps are usually connected to a wireless network. The network allows the pump to connect to a backend server to collect metadata, and it permits wireless updating of drug libraries and firmware. In some cases, the network also allows interaction between the pump and the electronic health record for one-way or two-way communication. Additionally, infusion pump vendors can log in remotely to troubleshoot and collect data on the pumps.

• Now that infusion pumps are network-enabled, they can be hacked by third parties or, like other medical devices with operating systems and software that connect them to a network, infected by malware, which can cause them to malfunction or operate differently than originally intended.

• Traditional security scan techniques can adversely affect the devices. Manufacturers often consider upgrades to software as a change to the device itself that requires further certification, such as Food and Drug Administration (FDA) 510(k) clearance.

Even though FDA officials have said it is not necessary to go through recertification, manufacturers are reluctant to make upgrades without further testing the devices.

• Manufacturers do not want to retest because the devices' internal processes are costly and unmodifiable. There is no streamlined process for testing upgrades or performing partial testing. Manufacturers must perform the full suite of tests regardless of the type of change.

• Most infusion pumps have maintenance and clinical-use usernames and passwords that are hard-coded. This system creates security problems, such as an inability to revoke access codes when an employee leaves the hospital.

The full NIST report is available at http://tinyurl.com/m5eaqav. ■

Anthem breach traced to admin's stolen login

The data breach at Anthem, one of the country's most prominent health insurers, is thought to be the largest healthcare data breach in history by a wide margin. The insurer is reporting that the breach affecting 80 million people was traced to the theft of an administrator's login key and password.

The information stolen from the insurer giant includes names, birthdays, medical identifications, Social Security numbers, street addresses, e-mail addresses, and employment information, including income data, Anthem announced. The compromised database contained up to 80 million customer records. Anthem said the breach resulted from a "very sophisticated external cyberattack," and initial suspicions fell on China. The data were not encrypted.

Formerly known as Wellpoint, Anthem is the second-largest health insurer in the United States. The company operates plans including Anthem Blue Cross, Anthem Blue Cross and Blue Shield, Amerigroup, and Healthlink.

Anthem's investigation determined the hackers somehow obtained the credentials of five tech workers, possibly through a "phishing" scheme that could have tricked a worker into unknowingly revealing a password or downloading malicious software, said spokeswoman **Kristin Binns**. The company found unauthorized data queries with similar hallmarks as early as Dec. 10, and they continued sporadically until Jan. 27. Attempts also might have been made earlier in 2014, she said.

Anthem officials discovered the breach itself and announced it only a few days afterward. That timetable is not typical, and it shows that companies are learning the value of database monitoring and disclosing a breach immediately, says **Ken Westin**, a security analyst for Tripwire, a company in Portland, OR, that provides cyber security services. Members of the Anthem staff reported that they discovered the breach when a system administrator saw that his login credentials were being used by someone else to access the system.

"Once hackers are able to compromise a few high-level employee systems through a phishing campaign either through malware attachments or through a browser exploit, gaining access to a user's database credentials would be trivial," Westin explains. "This would be where the sophisticated malware that is being reported by Anthem would be utilized. If the malware was designed specifically for this attack, it would evade most anti-virus products."

A key weakness is that it appears there were no additional authentication mechanisms in place beyond the administrator's login and password or key to prevent access to the entire data warehouse, Westin says. Anthem's primary security sin might not have been the lack of encryption, but instead improper access controls, he says.

Encryption is always advised for protecting data even when a system is breached, but Westin points out that if the attackers had administrator-level credentials, encryption would have been moot anyway. The same credentials that got the hackers into the system would allow them to decrypt the data. *(See the story on p. 34 for more on how to prevent data breaches.)* "The Anthem case also shows the importance of monitoring database activity," Westin says. "If the admin had not noticed his credentials were being used, it may have taken longer for Anthem to respond, and additional data could have been compromised." ■

Experts advise compliance not same as security

The data breach at Anthem holds important lessons for risk managers, say four cyber security experts consulted by *Healthcare Risk Management*.

The Anthem breach and other recent incidents demonstrate that "compliance does not equal security," says **Ulf Mattsson**, chief technology officer at Protegrity, a Stamford, CT-based provider of enterprise data security software and services. "We strongly urge healthcare organizations to not only follow regulatory security rules, but to go beyond them, as they are just a baseline or minimum of acceptable security."

The sophistication of attacks continues to grow, says **Steve Hultquist**, chief evangelist at RedSeal, a security analytics company in Sunnyvale, CA. Attackers are using increasingly powerful automation to probe for and attack weaknesses through the network of connected systems. "Ensuring that the dizzying complexity of modern networked systems reflects the intended security architecture and plan is impossible without defensive automation that both protects and analyzes those defenses," Hultquist says. "Without daily analysis, organizations are left hoping that their systems are operating as they intend, and we're learning that any such hopes are in vain."

The information stolen from Anthem includes key pieces of data that can be used to access someone's financial records or steal a person's identity, notes **Eric Chiu**, president and co-founder of HyTrust, the cloud control company in Mountain View, CA. "These type of attacks are often extensive in terms of the amount of information bad guys are able to pilfer, because they typically happen from the inside using system administrator or employee credentials," he says. "Organizations need to make security a top priority and think of it as part of doing business. Otherwise, we will continue to see these breaches happen, and consumers will continue to suffer because of them."

Martin Walter, senior director at RedSeal, agrees that a breach of a healthcare organization's records could be worse than a typical company having credit card numbers stolen by hackers. Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times more on the black market, he explains.

"The interesting thing here is comparing the value of this information to the spending on security in the healthcare sector, which is disproportional. Credit card information in retail tends to be better protected than personally identifiable information and Social Security numbers in healthcare, even though it's less valuable in terms of selling price," Walter says. "It was only a matter of time until hackers found out that it's much easier to go after Social Security numbers and personally identifiable information with healthcare providers, which in comparison spend significantly less on security, making them tentatively easier targets."

SOURCES

- **Eric Chiu**, President & Co-founder, HyTrust, Mountain View, CA. Telephone: (408) 776-1400.
- **Steve Hultquist**, Chief Evangelist, RedSeal, Sunnyvale, CA. Telephone: (408) 776-1400.
- **Ulf Mattsson**, Chief Technology Officer, Protegrity, Stamford, CT. Telephone: (203) 326-7200. ■

Settlement for misdiagnosing first U.S. Ebola patient

Texas Presbyterian Hospital in Dallas announced recently that it has settled with the family of Thomas Eric Duncan, the first Ebola patient diagnosed in the United States.

"As part of the healing process, we have again extended our sincere apologies to the family and shared our regret that the diagnosis of Ebola Virus Disease was not made at the time of Mr. Duncan's initial Emergency Department visit," Texas Presbyterian Hospital said in a statement.

In addition to a financial settlement, the hospital will create a charitable organization in Duncan's name. Neither party divulged the amount of the settlement, but Texas caps malpractice awards for pain

COMING IN FUTURE MONTHS

- Health passports: Hidden risks?
- Reducing misplaced NG tubes
- Triple Aim improves safety
- Latest on OR fire safety

and suffering against a physician at $250,000 and damages against hospitals at $250,000 per hospital.

A representative for the Duncan family at a press conference announcing the settlement retracted previous allegations that the patient was treated poorly because of his race. The hospital recently provided information to *The Washington Post* and said that the initial news reports of Duncan's first visit to the emergency department were misleading.

A hospital spokesman stated that Duncan told staff members he had been in Africa, not specifying West Africa, which would have triggered Ebola suspicions. In addition, Duncan's fever was not 103 degrees, which is the threshold for Ebola protocols, when he first arrived, the spokesman said. His initial temperature was 100.1 degrees, but it rose to 103 degrees while he was present, the hospital spokesman said. *(For more information on Ebola and the Duncan case, see* Healthcare Risk Management*, December 2014, pp. 121-129.)* ■

Malpractice suit filed in Joan Rivers' death

Melissa Rivers filed a malpractice lawsuit recently against doctors and the clinic where her mother, Joan Rivers, died after a routine medical procedure.

The lawsuit alleges doctors mishandled the endoscopy and performed a laryngoscopy on her vocal cords without consent. It also claims the doctor left the operating room to avoid being caught.

"To put it mildly, we are not just disappointed by the acts and omissions leading to the death of Joan Rivers, but we are outraged by the lack of care and concern for Ms. Rivers on the part of her treating physicians and the endoscopy center where the treatment was rendered," says a statement released by Rivers' attorneys, **Jeffrey Bloom**, JD, and **Ben Rubinowitz**, JD, both in New York City.

The Centers for Medicare and Medicaid Services (CMS) investigated after the death and found the Yorkville Endoscopy clinic made several errors, including failing to get informed consent for every procedure performed and failing to record Rivers' weight before the administration of sedation medication. CMS also said the clinic failed to keep proper medication records and personnel took cell phone photos of Rivers while she was unconscious.

CMS announced on Jan. 9 that the clinic failed to correct the deficiencies and would be banned from receiving Medicare and Medicaid reimbursement. "After a careful review of the facts, Yorkville Endoscopy L.L.C. no longer meets the conditions of coverage for a supplier of Ambulatory Surgical Center (A.C.S.) services," said the letter from CMS. Medicare and Medicaid participation was terminated on Jan. 31.

Melissa Rivers said in a statement that she filed the malpractice lawsuit because "[t]he level of medical mismanagement, incompetency, disrespect and outrageous behavior is shocking and frankly, almost incomprehensible." ■

Manual helps to improve medication reconciliation

Unintentional medication discrepancies during transitions in care pose a major threat to patient safety, with up to 67% of inpatients having at least one unexplained discrepancy in their prescription medication history at the time of admission, according to the Society of Hospital Medicine (SHM) in Philadelphia.

One solution to this problem is medication reconciliation. SHM has developed a manual through an Agency for Healthcare Research and Quality grant to help hospitals improve medication reconciliation practices.

The Multi-Center Medication Reconciliation Quality Improvement Study (MARQUIS) identifies best practices for medication reconciliation processes throughout admission, transfer, and discharge.

The MARQUIS Implementation Manual is available for free on the SHM website at http://www.hospitalmedicine.org/MARQUIS. ■

CNE OBJECTIVES

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

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

HEALTHCARE RISK MANAGEMENT™

CNE INSTRUCTIONS

To earn credit for this activity, please follow these instructions:
1. Read and study the activity, using the provided references for further research.

2. Scan the QR code to the right or log on to the new AHCMedia.com site to take a post-test. Go to "MyAHC" and then "My Courses" to view your available CE activities. Tests are taken after each issue. First-time users will have to register on the site using the 8-digit subscriber number on their mailing label, invoice, or renewal notice.

3. Pass the online tests with a score of 100%; you will be allowed to answer the questions as many times as needed

4. After completing the test, your browser will be automatically directed to the activity evaluation form, which you submit online.

5. Once the completed evaluation is received, a credit letter will be e-mailed to you instantly.

CNE QUESTIONS

1. In the case of a nurse who made a fatal medication error at St. Mary's Hospital, in 2007, what scheduling scenario was thought to cause her inattentiveness?

A. She worked her regular eight-hour shift, an extra shift that same day, then her regular 7 a.m. shift the next day.
B. She worked two back-to-back 12-hour shifts.
C. She worked only her regular eight-hour shift but had been unable to sleep the night before.

2. According to the Health Care Workers Compensation Barometer report from Aon Risk Solutions, which of the following is true?

A. 65% of survey respondents have a return-to-work program, and 90% have metrics in place to test the effectiveness of the program
B. 90% of survey respondents have a return-to-work program, but only 65% have metrics in place to test the effectiveness of the program
C. Nearly all hospitals have a safety incentive program in place.

3. According to Linda Zdon, director of information security and compliance at Allina, what is one reason it is difficult to secure infusion pumps as a gateway to a data breach?

A. All infusion pumps from the same vendor have the same login and password.
B. Vendors prohibit hospitals from altering software related to the infusion pump.
C. Infusion pumps use underlying software systems that are unfamiliar to hospital network engineers.

4. According to CEO Nick Merkin of Compliagent, why can nurse fatigue be a compliance issue?

A. Patients might report unsatisfactory care to state nursing boards.
B. Many states require healthcare facilities to maintain minimum staffing levels as a ratio of nursing hours per patient day or other metrics.
C. Federal law prohibits 12-hour shifts.

LEGAL REVIEW & COMMENTARY
EXPERT ANALYSIS OF RECENT LAWSUITS AND THEIR IMPACT ON HEALTHCARE RISK MANAGEMENT

Jury awards verdict of $5.2 million after diagnosis error and above-the-knee amputation

'High-low' agreement reduces verdict to $1.5 million

By Damian D. Capozzola, *Esq.*
Law Offices of Damian D. Capozzola
Los Angeles

Jamie Terrence, *RN*
President and Founder, Healthcare Risk Services
Former Director of Risk Management Services (2004-2013)
California Hospital Medical Center
Los Angeles

Tim Laquer, *2015 JD Candidate*
Pepperdine University School of Law
Malibu, CA

News: The patient, a 49-year-old man, was accidentally injured by a collapsible barrier that raised while the man was walking over it, which trapped his left leg and twisted it. His knee was momentarily dislocated in the process, and the patient was taken to a nearby hospital emergency department. A physician's assistant (PA) evaluated the patient and noted serious symptoms including numbness of the leg, paresthesia, and sharp pain. The PA ordered an X-ray and subsequently diagnosed a simple knee sprain. A physician in the emergency department agreed with the PA's findings and diagnosis, and the patient was discharged. Two days later, the patient returned to the hospital and had no feeling in his left foot. It was then discovered that the patient had torn ligaments and tendons, and he suffered a tear in his popliteal artery. The patient underwent an above-the-knee amputation. The patient brought suit against the hospital, PA, and physician, and he alleged that the incorrect diagnosis caused his injury. The defendants all denied liability. The jury agreed with the patient and awarded $5.2 million in damages against all three defendants, which was reduced pursuant to a "high-low" agreement.

Background: The patient was a 49-year-old man who was accidentally injured in December 2009 while leaving his job. A collapsible barrier was inadvertently raised while the patient was walking over it, and this action trapped and twisted the man's leg. His left knee was momentarily dislocated during this accident, and he was rushed to a nearby hospital emergency department via an ambulance. At the hospital, the patient was evaluated by a PA. The PA recorded serious symptoms in the patient's medical chart, including leg numbness, paresthesia (tingling, prickling, or other skin sensations), and sharp pain. The patient also reported an inability to move his left foot. The PA ordered an X-ray of the leg and diagnosed the patient with a simple knee sprain. The PA did not evaluate the patient's range of movement in his leg or order further tests beyond the X-ray. A physician in the emergency department testified that she agreed with the PA's findings and diagnosis, but it was unclear at the trial whether the physician evaluated the patient. The patient's medical chart provided no evidence of an evaluation, and the physician did not sign the medical chart until 10 days after the patient's hospital visit. The patient was discharged with instructions to see an orthopedic surgeon.

However, two days after his discharge, the patient returned to the same hospital complaining of the same numbness, pain, and lack of feeling in his left foot. At this point, it was discovered that the patient had torn nearly all of the ligaments and tendons in his knee, and the knee

Financial Disclosure: Author Greg Freeman, Executive Editor Joy Daughtery 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. Damian Capozzola, Jamie Terrence and Tim Laquer, co-authors, have no relevant relationships to disclose.

dislocation had caused a tear in his popliteal artery. These injuries kept the leg from receiving enough blood, which resulted in the tissues in his leg and foot dying. The hospital attempted to save the leg, but this attempt ultimately was unsuccessful. The patient had no option but to undergo an above-the-knee leg amputation.

The patient brought suit against the hospital, the PA, and the physician. The patient claimed that the initial incorrect diagnosis constituted a deviation from the appropriate standard of care and, thus, was medical malpractice. According to the patient and his experts at trial, the PA, and the physician herself, should have performed additional diagnostic tests to rule out an injury to the popliteal artery. One expert, a vascular surgeon, testified that these tests would have revealed the injury to the artery and it could have been repaired at that time, thus the delay in diagnosis caused blood depravation to the leg and foot that necessitated an amputation. The defendants attempted to argue that their actions met the standard of care, although the PA admitted that she suspected a knee dislocation. After three hours of deliberation, the jury found the defendants jointly and severally liable and awarded $5.2 million in damages. However, the parties had previously negotiated a "high-low" agreement that guaranteed the patient recovery of at least $750,000 but no more than $1.5 million. As a result of this agreement, the $5.2 million verdict was reduced to $1.5 million.

What this means to you:
Diagnostic errors account for a large number of medical malpractice cases every year, and these claims can result in particularly large verdicts. As with other types of errors, a misdiagnosis or failure to diagnose is viewed in accordance with the applicable standard of care: how a similar physician or healthcare provider would have acted under the same or similar circumstances. A physician is not necessarily negligent because of an error in judgment or because efforts ultimately prove unsuccessful. However, if a medical issue is common or well-known in the medical community, and diagnosis of that issue is similarly commonplace, then a physician who fails to diagnose the issue or improperly diagnoses a different issue might be liable for medical malpractice, if a reasonable physician in the same or similar circumstances would be able to properly identify the issue.

Ordering and performing the appropriate diagnostic tests is a critical part of this process and is the major issue for the physician and PA here. Popliteal artery tears are not uncommon and should be suspected, especially after an injury that also involves a dislocation. Bone fragments as well as twisting injuries can sever this artery. Initial symptoms are commonly numbness and tingling as a result of diminished blood supply to the area the artery serves. The injury can be further exacerbated if the knee is not immobilized and the patient continues to bear weight on it. A simple check of pedal pulses, a routine examination done for this type of injury, would have revealed a compromised vascular system below the injury. A CT scan would be the standard diagnostic test for a patient with this injury and accompanying symptoms. The PA in this case ordered only an X-ray, which was insufficient given a suspected knee dislocation, and that insufficiency was enough to rise to the level of medical malpractice.

The role of the PA can vary from one healthcare organization to another. The medical staff of each facility can determine the degree of independence of the PA as well as the areas of the facility in which they can function as long as state mandates are met. However, in all cases, the PA must practice under the supervision of a fully licensed physician. In this case, the PA admitted to having concerns about the patient's injury. The PA had a duty to consult with her supervising physician who, at that point, would have a duty to examine the patient, order additional tests, and consult with a vascular or orthopedic surgeon as well as a radiologist before even considering discharging the patient.

Life in the emergency department can be and often is hectic, fast-paced, and even chaotic at times. This situation requires extreme vigilance on everyone's part. Skipped steps and missteps can lead to devastating results for patients, healthcare organizations, and those who practice there. The ED physician's duties are lightened somewhat by support staff such as PAs or nurse practitioners. However, with the use of these assistants comes the added responsibility to supervise and document agreement with the care they provide.

Medical records and evaluations are of extreme importance for healthcare providers to protect themselves against medical malpractice claims. Keeping detailed and accurate records of a patient's medical procedures and evaluations by physicians, with comments relating to those evaluations, are critical in order to prove that these events occurred. In this case, the parties debated whether the physician evaluated the patient. If the physician did evaluate the patient, she failed

to note it on his medical chart. This lack of documentation makes it hard to prove at trial that the evaluation occurred. Meeting the standard of care is the most important part of treating a patient to prevent medical malpractice, but if there is no evidence to prove this, that situation will make the future difficult in proving that a medical care provider actually did comply with the standard of care.

This case also reveals how "high-low" agreements can be a powerful device for physicians and hospitals to reduce their potential liability. The agreement sets a minimum amount that the plaintiff will recover, even in the case of a defense verdict, but it also sets a maximum amount for recovery. Because juries are not informed of these agreements, there is not a fear that the jury will hear about it and automatically award the maximum. These agreements are beneficial to both sides. Plaintiffs have a safety net that guarantees some monetary recovery, and defendant physicians and hospitals can protect against runaway juries who issue huge verdicts. If a medical malpractice case arises and continues all the way to trial, physicians and hospitals should discuss with counsel about potentially negotiating a "high-low" agreement. It offers protection from enormous verdicts, with the cost of the agreement being some loss recognized.

REFERENCE:

Circuit Court for Baltimore City, MD. Case No. 24C12008071. May 23, 2014. ■

Failure to treat bacterial infection from routine injection results in $2.3M verdict

News: The patient, a 52-year-old man, unknowingly contracted a bacterial infection from a routine injection administered as part of the process for an MRI. He sought follow-up care related to the initial MRI procedure a few days later, and met with a physician at a hospital. A culture test was performed, and the physician had access to the test results, which revealed the bacterial infection. Despite these test results, the physician sent the patient home without any antibiotics or a definitive diagnosis after a 25-minute consultation. Two days later, the patient was rushed back to the hospital with crippling pain. The severe infection compromised the patient's tissue and bone in his hip, which resulted in him requiring a complete hip replacement procedure three months later. The patient brought suit against the consulting physician and the hospital, and he claimed that the physician should have identified and treated the infection based on the culture results. The defendants claimed they met the applicable standard of care. The jury found both liable and awarded the patient $2.3 million in damages.

Background: The patient was a 52-year-old man who worked in construction. In 2010, the patient underwent an MRI procedure that included a routine injection as part of the process. A few days later, he visited a hospital for follow-up care relating to the MRI and met with a physician, the head of the hospital's orthopedic surgery. The patient had a culture test performed that revealed a severe bacterial infection. However, the patient had a 25-minute consultation with the physician, who had the test results at this time but failed to diagnose the infection. The physician released the patient home without any antibiotics or any definitive diagnosis. Two days later, the patient was rushed back to the hospital with crippling pain, at which point the severe infection finally was discovered. By this point, however, the infection had spread throughout the patient's system, and the damage already was done. The severe infection compromised the patient's tissue and bone in his hip, and he required a complete hip replacement procedure three months after the infection. As a result of the infection, the patient was unable to resume his work in construction and suffered from limitations in his other daily activities.

The patient brought suit against the physician and the hospital, as the employer of the physician, and he alleged that the physician's brief consultation and failure to identify and treat the infection constituted a deviation from the standard of care. The patient did not bring suit against the parties responsible for causing the infection itself, despite the fact that they set the series of events in motion. It is unclear why this choice was made, but it is possible that the patient felt the subsequent failures were more significant and a more direct cause of the hip injury. The patient's primary allegations related to this point: The physician exacerbated an existing condition, the infection, rather than creating a medical condition. Accordingly, the patient and his experts believed that the infection could have been contained or treated sooner had the physician properly diagnosed it at that time.

The defendants claimed that, given the information the physician had at the time, his course of action fell within the appropriate standard of care. The jury agreed with the patient and found the physician and hospital jointly and severally liable. The jury awarded $2.3 million in damages.

What this means to you: The primary issue for the providers in this case was whether the failure to identify and treat an existing condition constituted a departure from the standard of care. The patient here did not seek recovery against the parties responsible for initially causing the infection, but rather targeted the physician and hospital that could have prevented the serious injury that occurred as a result of the infection. Once an individual becomes a patient, a provider owes that patient a duty to provide the appropriate standard of care, and the providers take the patients as they are. Exacerbating an existing condition can constitute negligence if a reasonable physician, given the same or similar circumstances, would not do such. The physician in this case was not initially responsible for the infection, but once the patient came under his supervision, he was responsible for treating that infection in accordance with the standard of care.

Healthcare-associated infections (HAIs) are quite common. According to the Centers for Disease Control and Prevention (CDC), based on a large sample of U.S. acute care hospitals, one in 25 hospital patients has at least one HAI. The CDC has established numerous guidelines for prevention and treatment of HAIs, including specifics for injection safety such as using aseptic technique in a clean area free from contamination. Most hospital-acquired bloodstream infections occur after insertion of a central venous catheter used for long-term administration of fluids and drugs. However, bacteria can enter the bloodstream after any type of intravenous procedure. If a patient complains of symptoms following this type of procedure, an infection should be suspected. Sepsis screening should be performed and is the standard of practice in hospitals today. Blood cultures are a vital clinical tool used to diagnose septicemia suspected after an intravenous procedure. The presence of bacteria in the bloodstream is considered a "critical value," and hospital and freestanding laboratories have protocols in place to immediately notify physicians of the test results. For more information, visit the CDC's website at http://www.cdc.gov/hai/index.html.

Physicians and healthcare providers must recognize that HAIs are common, and when they are treating a patient who recently has received healthcare services or undergone a procedure involving an injection, extra precautions should be taken to rule out the possibility of an infection. In this case, the hospital followed the proper procedure by ordering the culture test, which did reveal the presence of an infection. However, ordering the appropriate test or tests is only the first step in the course of treatment.

Following up after receiving test results is the next step and is critically important. Merely performing diagnostic tests does nothing to help a patient recover from an illness. It enables the physician or healthcare provider to properly diagnose the patient, but then the care provider must continue by prescribing appropriate medication, recommending and performing an operation, or providing whatever the appropriate treatment is based on the diagnosis. Because it can be days before some culture results are ready, physicians should be sure to have current contact information for patients so that the patient can be notified if positive test results are received after the patient has been to the physician's office. It is then the duty of the physician to quickly treat the patient for the infection. Any breach of this duty falls well below the standard of care and is negligent. A delay in treating a bloodstream infection can result in bacteria "seeding" around a heart valve or in a joint, with disastrous results.

Failure to treat an underlying condition can constitute medical malpractice in which there is deviation from how a reasonable physician, given the same or similar circumstances, would treat the condition. However, this analysis is dependent upon the condition and the patient. A physician cannot force a patient to receive treatment for an illness, but the physician has a duty to inform the patient of his or her options for treatment as well as the consequences of forgoing treatment. In certain situations, a patient might find the detriments of treatment to outweigh the benefits of that treatment. The patient has the knowledge to make the decision, and physicians fulfill their duty by giving the patients that knowledge. However, for a simple situation such as an infection, it is doubtful that a patient will refuse treatment given the simple nature of the treatment and minimal, if any, side effects or negative consequences of the treatment.

REFERENCE:

Supreme Court of Rockland County, NY. Case No. SU-2011-004050. June 4, 2014. ■