HEALTHCARE RISK MANAGEMENT™

35TH ANNIVERSARY

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

## INSIDE



AHC Media

OCTOBER 2014 Vol. 36, No. 10; p. 97-108

# Plaintiffs obtaining more records that were previously thought safe

*Judge notes the 'inexorable march to more disclosure'*

Plaintiffs in medical malpractice cases and other healthcare litigation continue to win access to risk management documents long considered privileged, including handwritten notes made in the course of an investigation. This dangerous trend means that risk managers should reassess their habits on document creation to avoid showing all their cards to the other side.

Risk managers have long depended on quality or peer review exceptions, depending on the state, and a specific safe harbor under the Patient Safety and Quality Improvement Act of 2005 that protected patient safety work product. That's changing now, and quickly.

The trend toward increasing disclosure of risk-management materials includes documents pertaining to investigations of incident reports and unanticipated outcomes. That change means fact-gathering as a result of an incident or other problem associated with potential patient harm might be subject to disclosure, which is a turnaround from what risk managers have known for years.

> ... FACT-GATHERING AS A RESULT OF AN INCIDENT OR OTHER PROBLEM ASSOCIATED WITH POTENTIAL PATIENT HARM MIGHT BE SUBJECT TO DISCLOSURE ...

In the latest example, a circuit judge in Newport News, VA, instructed a hospital to turn over internal risk management materials to a patient's lawyer (*George Rauchfuss v. Roger E. Schultz, MD, et al.*, Case No. CL1302754P-03). While the hospital argued these materials were protected, the judge ruled it was within the now-deceased patient's right to seek them, says **Patrick J. Hurd**, JD, senior counsel with the law firm of LeClairRyan in



**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 **Greg Freeman**,
(770) 998-8455.

Norfolk, VA.

"Procedurally, the hospital did exactly as expected. It filed a motion to quash the subpoena and complained that the materials were protected," Hurd says. "The judge, however, evaluated the materials and decided several pieces of information must be disclosed to the patient, including that a doctor's own note showed he had missed a radiologist's suggestion to check for cancer."

Courts are struggling to interpret the law with the growing use of electronic records and the intertwined computer systems of a modern hospital, Hurd explains. When most documents were on paper, it was easier to distinguish what was on the patient record and what was privileged under peer review or other protections. With the electronic record, those lines are blurred.

"They're wrestling with this, and it's been a continuum of decisions," Hurd says. "We're seeing decisions that more and more documents are hospital records made in the course of ordinary business and the facts – not opinions – should be available to the plaintiff. This is happening all over the country."

Perhaps the greatest risk from increased disclosure is that healthcare professionals and institutions will become reluctant to report patient safety incidents, says **Leilani Kicklighter**, RN, ARM, MBA, CPHRM, LHRM, a patient safety and risk management consultant with The Kicklighter Group in Tamarac, FL, and a past president of the American Society for Healthcare Risk Management (ASHRM) in Chicago. "People say that if we don't have confidentiality in healthcare organizations, no one is going to report," she says. "How will we keep accurate data on frequency and other trends? We may never notice that the same problem is happening once every week on every unit in the hospital, meaning you have a bigger problem than what people on that unit think is just minor."

The incident report will be most challenging for risk managers who want to avoid disclosure of those notes, Kicklighter notes. Other documents following an incident might be safe if investigations are conducted only at the behest of your attorney, because in most jurisdictions that would make the resulting document protected under attorney-client privilege, she says.

That distinction might mean making a quick call to the attorney to report the incident and asking

## EXECUTIVE SUMMARY

A trend in court rulings shows that plaintiffs in litigation against healthcare providers are gaining access to more documents that traditionally have been considered off limits. Access to those documents can be damaging for the provider, so risk managers might need to change practices that generate paperwork.

- Many of the documents in question were previously protected by the attorney-client privilege.
- Notes made immediately after an adverse event are among those that might be accessed.
- Records created on the instruction of your attorney still might be protected.

"Should I go out and investigate this?" When the attorney says "yes," Kicklighter says it provides a foundation for gathering information on the instruction of your counsel, which can make it protected.

Kicklighter also notes, however, that the trend toward more disclosure is not necessarily a bad thing for risk management because it promotes transparency and data sharing. She acknowledges, however, that those are benefits for healthcare in general, and individual decisions on document disclosure can have serious repercussions for the hospitals. (*For more on the potential benefits of increased document disclosure, see the story on p. 101.)*

Plaintiffs across the country have been whittling away at the evidentiary exclusions protecting healthcare organizations, and Virginia is at the center of the fight. Another example is a May 2014 ruling from the Circuit Court of Hampton, VA, which highlighted the potential discoverability of electronic medical record (EMR) audit trails and metadata. In addressing the plaintiff's attorney's request for the defendant hospital's policies and procedures, the judge in the Hampton case (*Eason v. Sentara CarePlex Hospital, Sentara Hospitals, et al*. No. CL12-470) went so far as to cite "an inexorable march to more disclosure" of risk management materials in healthcare litigation. A spokesperson for Sentara, a health system based in Norfolk, VA, declined to comment on the case. *(See the story below for details on another case involving disclosure of sensitive documents.)*

True to the judge's word, reports suggest these procedural tactics are becoming more commonplace in medical malpractice cases across the country, especially in the long-term health litigation arena, Hurd notes. In light of this trend, healthcare risk managers should make sure their training, policies, and procedures always stick to the facts, Hurd advises. *(See the story on p.100 for more on how to protect your documents.)*

Though he represents hospitals and other healthcare providers, another attorney in Hurd's firm is leading the fight for more disclosure. That fight makes Hurd privy to some of the maneuvering used to gain more access.

"He's trying to get at risk manager's questions, notes, and other things related to the review of a particular adverse event or unanticipated outcome," Hurd says. "The two main arguments are that it is just a hospital document created in the normal course of business and, therefore, need not be protected, or it's a medical record."

The medical record theory goes like this: A "medical record" is not just the actual record itself in which notes are made, but rather it includes all the meta data that went into the clinical decisions and actions. That theory means that everything with a digital connection to the patient record is part of the record and the patient is entitled to it.

"If you allow that theory, then handwritten records that were typed or printed out that related to entries reflected on the electronic record can become part of the record too," Hurd explains. "Plus, any evidence that the risk manager went into the record will prompt a demand for any risk management records created or changed after that date. The theory there is that what the risk manager saw in the record influenced the risk management documentation and that connection makes those documents part of the patient record."

**SOURCES:**

Patrick J. Hurd, JD, Senior Counsel, LeClairRyan, Norfolk, VA. Telephone: (757) 441-8931. Email: patrick.hurd@leclairryan.com.

Leilani Kicklighter, RN, ARM, MBA, CPHRM, LHRM, The Kicklighter Group, Tamarac, FL. Telephone: (954) 294-8821. Email: lkicklighter@kickrisk.net. ■

# Hospital, plaintiff fight over incident report

Medical malpractice plaintiff's attorneys are increasingly confident about obtaining potentially game-changing documents that risk managers assumed would never be seen by the other side. The attorneys at one site seeking malpractice plaintiffs recently discussed the Aug. 21, 2014, decision of the Supreme Court of Kentucky. In that case, the defendant hospital claimed a federal confidentiality privilege to refuse to provide the medical malpractice plaintiff with a copy of the incident report. The incident report was written by a surgical nurse at the defendant hospital concerning an elective surgery that resulted in the death of the patient.

The plaintiff obtained the incident report. MedicalMalpracticeLawyers.com provides this summary of the case:

The decision was not easily reached. As the Kentucky Supreme Court noted, the Patient Safety and Quality Improvement Act

of 2005 was enacted by the U.S. Congress to encourage healthcare providers to voluntarily associate and communicate privileged patient safety work product (PSWP) among themselves through in-house patient safety evaluation systems (PSES) and with and through affiliated patient safety organizations. The act provides a confidentiality provision establishing that "patient safety work product shall be confidential and shall not be disclosed," except as authorized by the act itself.

After a patient died as a result of complications from elective spinal surgery, her estate filed a medical malpractice and wrongful death case during which the estate sought to be provided a copy of the post-incident or event report generated by a surgical nurse through the defendant hospital's patient safety evaluation system. The defendant hospital alleged that the only post-incident report that existed was a report created through its patient safety evaluation systems and therefore was protected from discovery by the federal privilege for patient safety work product created by the act.

"BECAUSE THESE TYPES OF REPORTS ARE REQUIRED IN THE REGULAR COURSE OF THE HOSPITAL'S BUSINESS, THEY ARE ... GENERALLY DISCOVERABLE UNDER KENTUCKY LAW.

The plaintiff argued, however, that the act's definition of PSWP expressly does not include information that is collected, maintained, or developed separately, or exists separately, from a patient safety evaluation systems. Therefore, according to the argument, such separate information reported to a patient safety organization is not by reason of its reporting considered to be patient safety work product.

The Kentucky Supreme Court came noted that Kentucky administrative regulations provide that "administrative reports shall be established, maintained and utilized as necessary to guide the operation, measure of productivity and reflect the programs of the facility" and these reports "shall include: . . . ncident investigation reports; and ... [o]ther pertinent reports made in the regular course of business."

Because these types of reports are required in the regular course of the hospital's business, they are hospital records, and, therefore are generally discoverable under Kentucky law. ■

# Avoid disclosure: Just the facts, ma'am

With plaintiffs getting their hands on more and more documents that previously were off limits, the best way to avoid that danger is to be strict about separating fact and opinion, says **Patrick J. Hurd**, JD, senior counsel with the law firm of LeClairRyan in Norfolk, VA.

The facts might be discoverable for a plaintiff, so don't mix in your thinking about how or why the incident occurred, or anything else besides what actually happened. Opinions and analysis still have more protection from prying eyes, so don't unnecessarily give those away when you are required to hand over factual material.

"While the likes of mental impressions, conclusions, opinions, or legal theories can be redacted, you cannot assume that they will be," Hurd says. "If the purpose of an investigation is to gather facts in the wake of an incident, then the training, policies, and procedures should hew closely to that purpose, never straying into matters of conjecture or opinion."

Examples of the facts include the date of the occurrence, the diagnosis, the treatment provided, and the patient's outcome and progress. Squelch any tendencies to jot down your thoughts about why the incident occurred, any relation to past incidents, or possible corrective action. Keep those thoughts completely separate.

A standardized form can help you collect only the facts after an incident, says **Leilani Kicklighter**, RN, ARM, MBA, CPHRM, LHRM, a patient safety and risk management consultant with The Kicklighter Group in Tamarac, FL, and a past president of the American Society for Healthcare Risk Management (ASHRM) in Chicago. State laws vary on requiring incident reports, and some, such as F lorida, proscribe what data must be collected. That type of form, whether prompted by state requirements or not, can be an effective strategy, she says.

"If your state does not proscribe

what information you must have, you can develop an incident report form that provides the demographic information of the patient and other meaningful information like who the doctor was, where it happened, and so forth," Kicklighter says.

Risk managers also should gain a thorough understanding of how the electronic medical record can be accessed, what digital connections make that possible, and what electronic footprints are left after accessing the document.

Another important step is to ensure a clear demarcation between investigative fact-gathering and review or analysis related to opportunities for improvement of quality care and patient safety, Hurd says. "Healthcare organizations must preserve their ability to take factual information and place it in the hands of quality review organizations," he said. "This process necessarily involves evaluating, assessing, and even opining about how changes in policies, procedures, processes, training, education, and credentialing could improve patient safety and quality of care." ■

## Silver lining with increased disclosure?

Risk managers are justified in fighting to keep some documents confidential, but being forced to release them to the plaintiff does not necessarily signal a crisis for healthcare in general, says **Leilani Kicklighter**, RN, ARM, MBA, CPHRM, LHRM, a patient safety and risk management consultant with The Kicklighter Group in Tamarac, FL, and a past president of the American Society for Healthcare Risk Management (ASHRM) in Chicago.

The overall trend to more disclosure could have a silver lining, she says. By making more patient safety and investigative documents discoverable, the courts could be doing a favor for the industry by allowing other institutions to benefit from the shared data and experiences of adverse events, Kicklighter explains.

> ... ALLOWING OTHER INSTITUTIONS TO BENEFIT FROM THE SHARED DATA AND EXPERIENCES OF ADVERSE EVENTS...

Healthcare institutions and individual providers should tell the patient what happened, and facts should not be held back, Kicklighter says. To that extent, disclosure of factual information is not contrary to risk management ideals, she says.

"There is a school of thought, and I think it's not unreasonable, that asks why are we keeping information from the public and other healthcare organizations when we could share information across the board and help make things safer," Kicklighter says. "That may be little comfort for a risk manager who has to turn over documents in a malpractice case, but it might not be the end of the world for the healthcare community."

## Hospital thwarts infant abduction with training and technology

Infant abduction is one of those rare but terrible incidents that hospital risk managers prepare for but hope they will never be tested. A California hospital's preparation was tested recently when a man tried to take an infant without authorization, but staff members' training and technology combined to stop the kidnapper before he could even leave the building.

The incident began about noon on Saturday, Aug. 9, at O'Connor Hospital in San Jose, CA, when a father attempted to take his newborn son out of the hospital against his mother's wishes, says **Kathy Harlan**, CPHRM, CHC, CCEP, director of risk management and legal services at O'Connor. The mother and father were involved in an argument. The father jumped on the mother's bed and took the baby from her arms. He left the room, and the mother screamed for help as the father hurried down the hallway.

A physician working nearby saw the man and became suspicious, so she got up and followed the father. As the father walked toward an exit, he entered a "pre-alarm" that recently was configured at O'Connor. In addition to the standard alarm that sounds when a tagged infant is taken beyond a specified exit, this pre-alarm is activated when the infant is in an

area about 10 feet from the door. The pre-alarm gives the person carrying the infant, and also any staff members in the unit, a warning that the baby is approaching the exit but has not left yet.

O'Connor uses the Hugs infant protection system manufactured by Stanley Healthcare, based in Waltham, MA. (More information is available at the company web site: http://tinyurl.com/k43xrgk.) The pre-alarm component cost the hospital $15,200, in addition to the basic cost of the system, which the hospital does not disclose.

When triggered, the pre-alarm issues a verbal warning in three languages (English, Spanish, and Vietnamese) that says "Stop. Alarm will activate." The message is short so that it does not take long to say it in three languages. The pre-alarm is only local, so it does not activate any alarm or code throughout the hospital.

The purpose of the pre-alarm is two-fold, Harlan says. It serves as a low key warning to parents or staff members who might have accidentally stepped too close to the alarmed door, and it also gives staff an earlier start on responding to an abduction.

The father triggered the pre-alarm, which brought nursing staff to join the physician. When the father proceeded to the exit, the staff members and physician called out for him to stop. He went through the door, which automatically activated the Code Pink alarm throughout the hospital.

The heads-up from the pre-alarm enabled the staff members and physician to react quickly, and the seconds it saved might be why the father did not get away with the baby, says **John Hryndej**, manager of safety and security at O'Connor. As staff members throughout the hospital responded to the Code Pink, they followed their training and proceeded to designated doors, stairwells, and elevators to stop the abductor. Staff members are instructed to confront the abductor, verbally commanding him or her to stop and hand over the baby, and notify security of their location. If necessary, they are instructed to surround the abductor and impede any effort to leave until security officers arrive to detain the person.

At the same time staff were taking their positions, the physician and nurses from the unit followed the father out to the elevator lobby. When they got there, other staff members already had stationed themselves at the elevator doors.

"They ended up encircling him, and one of the nurses took the baby from his arms," Hryndej says. "Security was there immediately and took him into custody, taking him to a private area to await the arrival of the police, who responded promptly."

The police arrested the father. Initially the police and hospital security agreed that they would take the father's armband that gave him access to the maternity floor and issue a trespass notice barring him from hospital property. However, a police officer subsequently returned from interviewing the mother and reported that she had scratches on her arms. Police officers then arrested him for domestic violence and child endangerment.

The unit's nursing supervisor immediately notified Harlan and **Pamela Brotherton-Sedano**, MS, RN, vice president of patient safety and corporate responsibility officer, who were off duty for the weekend. The on-duty security supervisor notified Hryndej.

As risk manager, Harlan sits on the hospital's safety committee and was directly involved in the decision to install the pre-alarm system. O'Connor Hospital requires infant abduction prevention training at new employee orientation and at annual competency reviews. Employees are trained on emergency codes, including Code Pink for an infant abduction, and how to respond. The hospital also performs two Code Pink drills per year.

Risk management is heavily involved in all training and preparation for a Code Pink, Harlan says When a Code Pink is called, she works directly with the unit supervisor to learn what she can about the circumstances of the abduction. The hospital's incident command center is opened to oversee the Code Pink.

"My primary responsibility, in conjunction with security, is to make sure the area where the abduction happened is not compromised until

## EXECUTIVE SUMMARY

A California hospital recently was successful in stopping an infant abduction before the kidnapper left the hospital. Hospital leaders attribute the success to a combination of good technology and staff training.

- The infant security system included an early warning alert that a baby was nearing a secure exit.
- The early warning allowed staff members to react faster than if only the exit alarm sounded.
- Staff confronted the man before he could leave the building.

authorities arrive to investigate," she says. "We also organize an administrative team to oversee issues like what is going to be communicated to the public and by whom."

Harlan also notifies the hospital's insurers and brokers. Other notifications, such as to the Centers for Medicare and Medicaid Services, The Joint Commission, and the state department of health are handled by Brotherton-Sedano. "Even though there was a happy ending, we still notified the Department of Public Health because it's an unusual occurrence," she says. "California law requires that we notify them of certain unusual events, and sometimes we notify them just to be on the safe side."

The hospital held a debriefing on Monday with everyone involved and administrators.

Harlan credits the pre-alarm system and the hospital's staff training with thwarting the abduction. "We were glad to see that our people were well-prepared and responded in just the way we hoped they would. Because they were alert and knew exactly what to do, the infant didn't get far from the unit," Harlan says. "But it also reminded us that we can never let our guard down. These things do happen, and they can be tragic if you're not prepared for them."

The lesson learned from the experience? "Drill, drill, drill," Harlan says. (*For recent coverage of infant abduction prevention, see* Healthcare Risk Management*, August 2914, pp. 73-76.)*

### SOURCES


Kathy Harlan, CPHRM, CHC, CCEP, Director of Risk Management and Legal Services, O'Connor Hospital, San Jose, CA. Telephone: (408) 947-2626. Email: kathyharlan@dochs.org.

John Hryndej, Manager of Safety and Security, O'Connor Hospital, San Jose, CA. Telephone: (408) 947-2626. Email: johnhryndej@dochs.org.

Pamela Brotherton-Sedano, MS, RN, Vice President of Patient Safety and Corporate Responsibility Officer at O'Connor Hospital, San Jose, CA. Telephone: (408) 947-2626. Email: pamelabrotherton@dochs.org. ■


# Hackers grab 4.5 million patient IDs from system

A Tennessee-based health system is learning the hard way that protecting patient data is a never-ending job.

In addition to the now almost routine incidents of employees losing laptop computers or hard drives, hospitals are facing off with determined and sophisticated computer hackers.

Community Health Systems (CHS), which operates 206 hospitals across the United States, announced recently that hackers recently broke into its computers and stole data on 4.5 million patients, including their names, Social Security numbers, physical addresses, birthdays, and telephone numbers. The breach affected all patients who received treatment from a physician's office tied to a network-owned hospital in the last five years and even those who only were referred there by an outside doctor.

The breach is the largest healthcare data loss to date related to hacking, and it takes the number two spot on the Health and Human Services "Wall of Shame" tracking healthcare data breaches affecting more than 500 people. *(For more on the Wall of Shame, see the story on p. 105.)*

## Not all the news is bad

In one bit of good news, the hackers did not access information related to patients' medical histories, clinical operations, or credit cards. The lost personal information, however, is protected by the Health Insurance Portability and Accountability Act (HIPAA). At least in theory, state attorneys general could sue CHS for damages. Patients also could sue the hospital network for negligence, if state law allows that action.

CHS has hospitals in 28 states, with most being in Alabama, Florida, Mississippi, Oklahoma, Pennsylvania, Tennessee, and Texas. Computer security professionals hired by CHS determined the hackers were in China and used high-end, sophisticated malware to launch the attacks, the health system reported.

The hospital network's announcement noted that it had removed the hackers' malware from its computer systems and implemented protections to prevent similar break-ins. In addition, CHS is offering fraud protection services to all the affected patients. (*See the story on p. 105 for more on CHS's investigation.)*

The consultants and the FBI told hospital officials that the hackers previously were known for corporate espionage and targeted valuable information about medical devices. The FBI said it is committing serious

resources to tracing the hackers. The huge breach prompted the FBI to warn healthcare organizations that hackers are targeting them. *(See the story below for more on the FBI warning.)*

After CHS announced the breach, it tried to address concerns about the financial effect. In a filing with the Securities and Exchange Commission (SEC), CHS stated that it "carries cyber/privacy liability insurance to protect it against certain losses related to matters of this nature."

This data breach is noteworthy because of its enormity, says **R. Stephen Trosty**, JD, MHA, CPHRM, president of Risk Management Consulting in Haslett, MI, and a past president of the American Society for Healthcare Risk Management (ASHRM) in Chicago. "You might say that the difference between other computer hacking and hacking hospital data is the number of files obtained and the amount of data for each patient," Trosty says. "However, I am not sure that there is anything that can be done to completely protect against this as long as there are clever, determined hackers who are determined to obtain the information."

The case is interesting because the scope seems to be far greater than other data breaches, and it also involves hospitals throughout the country, Trosty says.

The CHS experience should prompt risk managers to be certain that their hospital or system has the best possible firewalls, encryption, and use of passwords that are possible, Trosty says. "It is important that all hospitals take this threat seriously and have competent, educated people who establish, update, and enhance all data protections. It is important that this be regularly reviewed to be certain that it is meeting the most stringent possible criteria," he says. "It also is important to try to install protections that are best able to detect potential bugs."

Risk managers also should look at the firewall, encryption, and password protections that exist for data that is transferred from physician office practices and clinics to the hospital and any data that might then be transferred back to physician offices and clinics, Trosty advises. It is not enough to only look at data that is generated by the hospital.

There also should be an effort made to ensure that hospital-based and hospital-owned physician practices and clinics have installed the necessary protections within their own data systems, he says. The protections should exist internally within these entities (physician office practices and clinics), as well as between the hospital and the entities.

"It also is important that if a breach is discovered, immediate action is taken to correct the breach and install software that will prevent this type of breach from happening again," Trosty says. "The hospital must take corrective action relative to the breach and type of breach that has occurred. At the same time, there needs to be timely notification of patients whose data has been compromised."

## EXECUTIVE SUMMARY

A Tennessee health system is the victim of what might be the largest theft of patient information. Hackers obtained names, addresses, Social Security numbers, and other information on 4.5 million patients.

- The hackers used sophisticated technology.
- The FBI has warned healthcare institutions of the risk posed by hackers.
- Determined hackers are far more difficult to stop than the casual thief or inattentive staff.

### SOURCE

R. Stephen Trosty, JD, MHA, ARM, CPHRM, President, Risk Management Consulting, Haslett, MI. Telephone: (517) 339-4972. Email: strosty@comcast.net. ■

# FBI warns of hacker threat

The FBI has warned healthcare industry companies that they are being targeted by hackers, following a successful attack on Community Health Systems in Franklin, TN, that resulted in the theft of millions of patient records.

"The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)," the agency said in a *Flash* alert sent to hospitals and other providers. "These actors have also been seen targeting multiple companies in the healthcare and medical device industry typically targeting valuable intellectual property, such as medical device and equipment development data," the

alert said.

The FBI and Department of Homeland Security periodically release alerts to provide United States businesses with technical details and other information they can use to either prevent or identify cyber attacks. The reports are typically only issued to businesses and not distributed to the general public.

This alert was the second recent one for healthcare providers. In April 2014, they warned the industry that its systems were lax compared with other sectors, which makes it vulnerable to hackers looking to access bank accounts or obtain prescriptions. ■

## 'Advanced, persistent' hackers hit hospital system

After hackers obtained 4.5 million files on its patients, Community Health Systems (CHS) in Franklin, TN, filed a statement with the Securities and Exchange Commission (SEC) to address concerns that the incident might affect the publicly traded hospital chain's value.

There was no immediate decline in CHS' stock value, but the first class action lawsuit was filed against CHS in Alabama within hours of the system announcing the breach.

The statement to the SEC gives some insight into what CHS found out about the cyber attack.

CHS reported that its cyber forensics consultants determined the hacker or hackers had stuck in April and June 2014 and were an "advanced persistent threat" originating from China.

The cyber experts found evidence indicating that the hackers found vulnerability in a computer system serving CHS' physician practices but apparently that did not allow access to financial data such as credit card numbers. The hackers took what they could: the names, addresses, Social Security numbers and other demographic data on 4.5 million patients. ■

## Most data breaches tied to theft

The Department of Health and Human Services' (HHS') database of major breach reports, those affecting 500 people or more, has tracked 944 incidents effecting personal information from about 30.1 million people, the government agency reports.

Most those records are the result of theft (17.4 million people), followed by data loss (7.2 million people), hacking (3.6 million), and unauthorized access accounts (1.9 million people). The recent breach at Community Health Systems in Franklin, TN, boosts the total number of records lost by 4.5 million. (The list is online at http://tinyurl.com/breachtool.)

In smaller breaches affecting fewer than 500 people, HHS received 21,194 reports of smaller breaches affecting 165,135 people in 2012, according to the department's most recent report to Congress. (That report is available online at http://tinyurl.com/breachreports.) ■

## Criminal charges for hospital execs in Georgia whistleblower case

A whistleblower's allegations have sparked a wide-reaching investigation of alleged fraud by four hospitals in Georgia, and two executives have pleaded guilty to conspiracy.

The whistleblower's civil lawsuit contends a prenatal clinic, Clinica de la Mama, was paid to refer clients to Hilton Head (SC) Hospital and four Georgia hospitals for Medicaid-paid deliveries. Tenet Healthcare Corp., which owns Hilton Head Hospital, and Health Management Associates (HMA), the Georgia hospital company, conspired with Clinica de la Mama to generate Medicaid revenue by targeting illegal immigrants, the suit said. The suit also claims Hilton Head Hospital paid the clinic for these referrals.

Gary Lang left Hilton Head in 2007 to become CEO at Clearview Regional Medical Center in Monroe, GA. The civil lawsuit and criminal charges claim he duplicated the referral practice there. "These illegal referral arrangements resulted in women being steered to deliver their babies at hospitals on the basis of Clinica's and the hospitals' financial self-interest, regardless of whether it was in the women's best interest," U.S. Attorney **Sally Quillian Yates**, JD, said in a news release.

Lang pleaded guilty to conspiracy

## EXECUTIVE SUMMARY

Four hospitals in Georgia are under investigation for allegedly paying kickbacks to attract pregnant Medicaid patients. The case originated with a whistleblower.

- Two executives pleaded guilty to criminal charges.
- The hospitals are accused of recruiting pregnant illegal aliens.
- The hospitals could face fines of hundreds of millions of dollars.

to violate an anti-kickback law and will enter into a plea agreement with the U.S. Attorney's Office, according to court documents. Lang face a maximum penalty of five years in prison and a fine of $250,000. His negotiated plea deal will be issued Jan. 15, 2015.

Co-conspirator Tracey Cota, chief operations officer of Clinica de la Mama from 2000 to 2010, pleaded guilty to the same charges. In court filings, the hospitals argued they had legitimate business relationships with the prenatal clinics and the referrals were the result.

The civil lawsuit is ongoing. The state of Georgia and the federal government joined the civil case, and now the hospitals could face hundreds of millions of dollars in penalties. Tenet Healthcare has faced allegations of improper billing in the past. In 2012, it agreed to pay $42.7 million to settle a Medicare overbilling case. In 2006, it agreed to pay more than $900 million over four years to settle another federal case involving improper billing.

**Marlan Wilbanks**, JD, partner with the Atlanta law firm of Wilbanks & Bridges, represents whistleblower Ralph D. "Bill" Williams. Wilbanks' firm focuses on representing whistleblowers. In another case handled by the firm, *U.S. v. Halifax Hospital Medical Center et al.,* whistleblower Elin Balid-Kunz gained inside knowledge from more than 17 years of employment at Halifax Hospital in Daytona, FL, and is presently the Halifax director of physician services. In her whistleblower lawsuit, Kunz alleged that Halifax knowingly and intentionally submitted thousands of fraudulent claims to Medicare. Additionally, she alleges that Halifax paid kickbacks to key referring physicians to generate patient referrals to the hospital. On March 3, 2014, Halifax Health settled the Medicare kickback claims portion of this case for $85 million.

> "RISK MANAGERS NEED TO BE WORKING WITH THEIR COMPLIANCE OFFICERS ON ISSUES LIKE THIS."

In the case involving HMA, Wilbanks says it appears the two executives awaiting sentencing are cooperating with prosecutors. Wilbanks notes that the case involves "sham contracts" to provide prenatal services to patients. "They weren't really contracts to provide those services," Wilbanks says. "They really were cover so that referrals could be captured from these clinics as a feeder system from the clinics to these hospitals, where undocumented women would give birth and the services provided would be paid for by Medicaid. It was a ruse that would allow a steady flow of these undocumented women to the hospitals."

The scheme was profitable, Wilbanks explains, because the Medicaid reimbursement for deliveries is lucrative when the overhead is fixed.

The plan fell apart when Williams, CEO of one of the HMA hospitals, found a contract on his desk for his signature. The contract was the renewal of a previous agreement with Clinica de la Mama to pay for around-the-clock translators, Williams realized he had never seen a translator at the hospital. When he asked around, no one else had seen translators either, but he was told that the contract was a standard one that Tenet had used for years. More digging revealed that the translator contract was how the hospitals paid the clinic for referrals.

Williams expressed his concern. He said the hospital was receiving no benefits from a service that cost them $10,000 a month, and it was clearly illegal. HMA stopped the arrangement and had only been involved in it for a short time, Wilbanks says. For that reason, HMA will pay less in the end than Tenet, which had run the scheme for a decade, he says. "Tenet even ran a cost benefit analysis on this plan at some point and found that they were getting a 50% return on investment — a 50% return on what was supposed to be a cost center," Wilbanks says.

Risk managers should be on the alert for any contract that could be, in whole or in part, a method of laundering money used for kickbacks

or other illegal acts, Wilbanks says. "They could have legitimately contracted for translation services or any other services from this clinic, but if even a part of that contract induces referrals for care paid with government benefits, that contract is illegal," Wilbanks says. "We're not saying no interpretation services were provided, but the contract was set up to provide cover for the checks that were going on a monthly basis to the clinic for referrals."

The plan also called for physicians with privileges at the hospitals to see patients at the Clinica de la Mama sites just before their due dates, supposedly as a free service for an underserved population.

"What they really were doing was getting their names and saying 'you're my patient now, and I have privileges at this hospital, and that's where you go when you're ready to deliver,'" Wilbanks explains. "The doctors benefitted with the fee to deliver the baby, and the hospitals benefitted from the Medicaid payment."

The case shows the need for a strong compliance program at the health system level and also at individual hospitals, says A**ndrew A. Oppenberg**, MPH, CPHRM, DFASHRM, director of risk management and patient safety officer at Dignity Health Glendale Memorial Hospital and Health Center in Glendale, CA.

"Risk managers need to be working with their compliance officers on issues like this," Oppenberg says. "There is a role for both compliance and risk management in preventing these kinds of arrangements, because you've made it clear that fraud like this won't be condoned, and also in spotting it if the deal is made anyway."

A solid compliance program should have uncovered a fraud scheme such as the one alleged with HMA, Oppenberg says. The whistleblower should not have been the first person to realize there were no translators in house, and there might have been others who were afraid to say anything, he says.

"An important part of a compliance program, and risk management too, is creating a culture in which this kind of activity is not tolerated," Oppenberg says. "Just as is important is instilling a culture in which people are not afraid to speak up when they see something wrong." ■

# Targeted interventions reduce med mal costs

A study published in the *Journal for Healthcare Quality* reports that many huge malpractice awards can be prevented by targeted interventions by healthcare provider organizations to reduce patient safety risks, such as reducing diagnosis errors.[1]

Despite the impact and influence of large malpractice payouts on healthcare costs, little is known about their specific characteristics and overall cost burden. Researchers at Johns Hopkins Medical Center in Baltimore reviewed all U.S. paid malpractice claims from 2004 to 2010 to identify key risk factors for catastrophic payouts, defined as claims of more than $1million. They represent 8% of all paid malpractice claims.

Results of their review showed that the greatest percentage of catastrophic payouts occur from errors in diagnosis. The authors noted that errors in diagnosis have twice the odds for a catastrophic payout and that health systems should focus more attention on ensuring diagnostic accuracy.

"Factors associated with catastrophic malpractice payouts present opportunities for targeted risk management and quality improvement efforts," says co-author **Martin A. Makary**, MD, MPH, a surgeon and professor at Johns Hopkins. *(For profiles of two cases with catastrophic payouts, see* Legal Review & Commentary *inserted in this month's issue.)*

The authors concluded that future studies should evaluate targeted interventions to improve patient safety in areas associated with catastrophic malpractice payouts, including efforts to improve diagnostic accuracy.

## COMING IN FUTURE MONTHS

- 'Hackathon' tests HIT security
- Corporate negligence in medical malpractice
- Fire prevention in the operating room
- Benefits of self-reporting to Joint Commission

## REFERENCE

1. Bixenstine PJ, Shore AD, Mehtsun WT, et al. Catastrophic medical malpractice payouts in the United States. J Healthcare Qual 2014; 36(4):43. ■

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 www.cmecity.com to take a post-test; tests are taken after each issue. First-time users will have to register on the site using the 8-digit subscriber number printed 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 to achieve a score of 100%.

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

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

# CNE QUESTIONS

1. **According to Leilani Kicklighter, RN, ARM, MBA, CPHRM, LHRM, with The Kicklighter Group, what is one to better protect the confidentiality of documents in an adverse event investigation?**

   A. Conduct investigations only at the behest of your attorney.
   B. Create documents only on paper.
   C. Immediately file all investigation documents with your in-house counsel or attorney.

2. **In the Aug. 21, 2014, decision of the Supreme Court of Kentucky regarding an incident report, what reasoning led the court to grant the plaintiff's request?**

   A. The report was discoverable because it was generated by a nurse on the unit in question
   B. Because the reports are required in the regular course of the hospital's business, they are hospital records, and, therefore generally are discoverable under Kentucky law.

3. **In the Community Health Systems' data breach, how did outsiders gain access to confidential patient information?**

   A. An employee lost a laptop computer.
   B. Outside hackers used high-end, sophisticated malware.

4. **In the case alleging a kickback scheme between a prenatal clinic and hospitals, how does the whistleblower allege the illegal payments were hidden?**

   A. In a contract for translation services.
   B. In a contract for vehicle maintenance.
   C. In a lump sum payment for physician services.
   D. In a bonus system tied to maternity referrals.

# 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.

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

# Family members awarded $16.7 million after radiologist missed evidence of lung cancer

*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 (2004-13)*
*California Hospital Medical Center*
*Los Angeles*

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

**News:** The patient, a 47-year-old woman, sought treatment at an ED in October 2006. She was complaining of a persistent cough. Her physician, a radiologist, ordered a chest X-ray in order to rule out pneumonia. When the physician read the X-ray, he determined that it was normal, and he diagnosed the patient with an upper respiratory infection. Barely a year later, the patient returned to the same hospital after her symptoms worsened. A different physician ordered a CT scan, which revealed signs of advanced stages of lung cancer. Within seven months, the cancer spread to other parts of the patient's body, which ultimately led to the patient's death in August 2008. The patient's only daughter brought suit on her mother's behalf against the initial physician and hospital. She alleged that the physician's failure to recognize a cancerous nodule in the initial X-ray was negligent. The defendants denied any wrongdoing. The jury found the physician and hospital jointly and severally liable, and it awarded the patient $16.7 million in damages.

MISDIAGNOSIS IS ... THE LEADING SOURCE OF SUCCESSFUL MEDICAL MALPRACTICE CLAIMS.

**Background:** In this case, the patient was a 47-year-old woman, a single mother with one daughter. The patient visited an emergency department at a hospital in October 2006, and she was complaining of a persistent cough. The physician in charge of treating her was a radiologist who ordered a chest X-ray in order to rule out pneumonia. After the physician examined the X-ray, he did rule out pneumonia, and he read the X-ray as normal. The physician diagnosed the patient with an upper respiratory tract infection, gave her prescriptions for antibiotics, and discharged her from the hospital.

Thirteen months later, the patient returned to the same hospital after the same symptoms worsened. At this second visit, a different physician ordered a CT scan, which revealed signs of advanced stages of lung cancer. At this point the patient finally was diagnosed with having lung cancer. The patient's health declined quickly. Within seven months of the new diagnosis, the cancer had spread to her liver, spine, kidney, and pubic bone, and the patient ultimately succumbed to the advanced cancer in August 2008.

The patient's surviving daughter brought suit against the radiologist and the hospital. She claimed that the physician failed to identify a nodule in the initial chest X-ray, and she said that this mistake constituted negligence. The plaintiff presented the 2006 X-ray as evidence, and medical experts during trial clearly identified a 1.5 cm nodule in the upper right lung of the patient. By 2007, this nodule grew to about 2.5 or 3 cm, and the later X-rays revealed several additional nodules that were not

**Financial Disclosure:** 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.

present in the first X-ray.

The defendants argued that the radiologist was able to see opaque areas in the chest X-ray, but these could have been caused by other things including tissue structures or other organs. Additionally, the radiologist argued that a chest X-ray is not the best tool for revealing lung cancer.

More importantly, the radiologist attempted to pass some of the blame to the patient herself by stating that he was not provided with the patient's full medical history. The patient was a smoker of 30 years, and her mother died of lung cancer, so the radiologist argued that without this vital information, his diagnosis could not have been completed correctly. Another attempted defense focused on causation. The defendants alleged that the patient's cancer was incurable at the time the radiologist became involved. The jury agreed with the plaintiff, found the radiologist and hospital liable, and awarded $16.7 million in damages.

**What this means to you:**
Misdiagnosis is a surprisingly common occurrence, and it is the leading source of successful medical malpractice claims. Radiology misreads (such as in this case) are classic and problematic. There is often subjectivity involved that can make litigation defense difficult.

It is unusual for a radiologist to be the first-line practitioner in an emergency department. A radiologist is usually called in to consult if radiological studies are ordered. It is highly unlikely that a radiologist would consult with another radiologist on a chest X-ray. The issue is safety, which stems from the specialist acting as the primary physician. Had an internist or family medicine or emergency department physician ordered the X-ray, there probably would have been a second read by a radiologist. Another consideration is that radiologists, not trained in emergency medicine, might not be as inquisitive about the patient's smoking history. It is a routine question asked in every emergency department. Make sure your emergency department staff members (nurses and physicians) obtain complete histories on all patients. They need to consider patients in denial who might exclude critical pieces of information out of fear. Finally, every patient receives discharge instructions which emphasize that they see their primary care physician in 2-3 days or come back to the emergency department if their symptoms don't improve or get worse. This discharge conversation not only needs to be said to patients, but it needs to be documented in the medical records.

More generally, an analysis of 25 years of data from the National Practitioner Data Bank revealed that diagnostic errors were the most common type (28.6%) and resulted in the highest proportion of payments (35.2%) in medical malpractice suits. Studies claim that delayed, missed, and incorrect diagnosis might affect 10-20% of cases, with potentially devastating results, as evidenced here. The radiologist in this case misdiagnosed the patient as having an upper respiratory tract infection that was far from the correct diagnosis of lung cancer. The plaintiff and her attorneys argued that this diagnostic error constituted medical malpractice and cost the patient her life. A 2009 report funded by the federal Agency for Healthcare Research and Quality (AHRQ) found that 28% of 583 physician-reported diagnostic errors were life-threatening or resulted in death or permanent disability, while only 31% were minor or insignificant.

Physicians should use as much relevant information as possible when diagnosing a patient in order to fulfill their duty to their patients. A patient's family and medical histories play a vital role in this diagnostic step, as this information can be a sign to the physician that this particular patient might have a unique background that makes the patient more susceptible to certain conditions. For example, knowing that a patient has been smoking for 30 years and her mother died of lung cancer would be likely to make the physician more cautious when examining a patient complaining of a persistent cough. A physician examining this patient could conduct a more thorough examination of the patient's lungs, or perhaps perform additional diagnostic tests, in order to determine if the patient has lung cancer.

This liability can blur between the physician and hospital, as hospital staff members might be responsible for asking patients for their full family and medical histories. However, it is the physician's duty to provide the appropriate standard of care to the patient, and a physician might be found negligent if a reasonable physician in the same position would inquire about the patient's history, despite any prior inquiry by staff. Asking patients these kinds of questions is simple and straightforward, with potentially huge consequences if left unanswered. Therefore, physicians and hospitals should ensure that they and their staff members are following through with these procedures.

Redundancies, such as having hospital staff members and physicians ask about a patient's history, might adversely impact efficiency in a

hospital setting where there are a large number of patients and employees, but redundancy can be a valuable tool for protecting against medical malpractice cases.

Having two sets of individuals perform the same task can reduce the likelihood that the task is overlooked, so if the task is critically important and has a potentially huge impact on the patient's care, then this redundancy might be worth the additional cost and sacrificed efficiency. This principle could have aided the case here beyond the patient's history as well. If a second physician had viewed the 2006 chest X-ray, that physician might have spotted the nodule which the first radiologist missed. Such a redundancy could have protected both the initial physician and the hospital, as the misdiagnosis could have been corrected shortly after it was made.

## REFERENCE

Suffolk County Superior Court, MA. Case No. SUCV2010-00558.June 18, 2014. ■

# Error during laparoscopic gallbladder surgery results in $1.5 million verdict for patient

**News:** The patient, a 30-year-old man, was admitted to a medical center in September 2010 for a laparoscopic gallbladder removal procedure. The procedure was performed by a surgeon with more than 20 years of experience. The surgeon severed an artery and vein while attempting to cut connective tissue covering the gallbladder. The surgeon continued and completed the gallbladder removal, but vascular surgeons were brought in for emergency vascular surgery. The patient survived but emerged with permanent neurological damage. The patient brought suit against the initial surgeon and the medical center, and he claimed that the surgeon's actions constituted medical malpractice. The defendants claimed that they exercised ordinary care during their treatment of the patient and that his injuries were from an unfortunate complication that is a known risk of laparoscopic surgery. The jury found the surgeon and medical center jointly and severally liable and awarded the patient $1.5 million in damages.

**Background:** The patient was a 30-year-old man who was studying aviation maintenance and had been a car mechanic, security guard, and amateur boxer. The patient suffered from gallstones, which were causing severe, sharp abdominal pain, but he otherwise was in healthy condition. He was admitted to a medical center in September 2010 for a laparoscopic gallbladder removal. The laparoscopic procedure typically involves the surgeon cutting four small openings in the abdomen to insert cannulas, narrow tube-like instruments, and a laparoscope, essentially a tiny telescope used to give the surgeon a view of the patient's internal organs. During the initial stages of the procedure, the surgeon pushed his blade through the patient's navel in one of the small incisions and sought tension from the fascia, a connective tissue that covers the gallbladder. When his blade met the tension, the surgeon began to cut. However, this tension was not from the fascia, but from an artery and vein, and the surgeon did not find out until after the cut was made. The surgeon had cut the patient's right common iliac artery and right iliac vein.

Once the surgeon discovered the mistake, he called for vascular surgeons to be brought in. The surgeon continued with the gallbladder removal while waiting the additional vascular surgeons, and the removal was completed without further complication. When the vascular surgeons arrived, they performed emergency surgery and managed to stabilize the patient. Unfortunately, the damage already was done. The patient emerged with permanent neurological damage and requires an electric stimulation device, which was implanted in his spine, to manage the pain from permanent nerve damage. The patient was unable to work in any of his previous occupations.

The patient brought suit against the surgeon and the medical center, which employed the surgeon. He alleged that the surgeon was negligent while performing the procedure and the medical center was responsible through the doctrine of *respondeat superior*, which means "let the master answer" and generally holds that an employer is responsible for the errors of an employee performed in the course of employment. Expert witnesses from the plaintiff and defense consisted of surgeons with a collective 15,000 gallbladder surgeries. These experts opined that cutting an artery or vein is a known possible complication of laparoscopic gallbladder surgeries, but during their surgeries, none of the experts had done so. Nevertheless, one expert who was publicized as a world leader in a particular type of surgery had cut an aorta while performing a surgery. The defense attempted to capitalize

on this situation and stated that the surgeon and medical center exercised ordinary care at all times and in all respects with regard to the treatment of the patient. After about eight hours of deliberation and a near-hung jury, the jury returned a unanimous verdict for the plaintiff. It found the surgeon and medical center liable for $1.5 million in damages.

**What this means to you:** The primary issue in this case was whether the surgeon fell below the standard of care while performing the incision and attempted cut of the fascia. Physicians and surgeons usually are proctored by other physicians with expertise in a procedure before they are permitted by hospitals to perform those procedures on patients. This step ensures hospital administrations that their patients will receive the best of care. Your own medical staff rules and regulations should address this step as it affords extra protection to patients and physicians as well as mitigating damages if an event occurs. The surgeon in this case appeared to have heavily relied on his past experience and expertise in attempting to defend himself. However, experience and expertise does not make a physician immune from negligence. Everyone make mistakes, even those who are the best at their profession.

Medical malpractice occurs when a physician fails to meet the applicable standard of care while treating a patient. In this case, the immediate action by the surgeon, once aware of the injury to the blood vessels, should have been to do a laparotomy, apply pressure over the area with clamps or sponges, and call for help. Continuing with the removal of the gallbladder was likely negligent, and the resulting loss of blood supply to the areas fed by the iliac artery became permanently damaged. Laparoscopic surgery has risks, and a common one is damage to blood vessels. Surgeons need to be especially cautious, as bleeding is not immediately evident through the laparoscope, and therefore should assess the patient's frequently for signs of internal bleeding. Physicians must be cautious to exercise the standard of care that another physician in the same or similar situation would exercise, regardless of how many years the physician has been practicing. Over time, this standard of care is constantly evolving with new developments in medicine and technology. Physicians thus must keep themselves up to date with such recent developments, especially as they gain traction and become more common in the field. If a new procedure or technique becomes normal, a physician who has been practicing 20 years must adapt and respond to these new changes, or risk facing questions about why the physician failed to perform similarly to other physicians given similar circumstances. However, "new" doesn't always mean "better,"so there can be debate and a potential for defense if an experienced physician performs a procedure while relying on known, proven techniques while eschewing newer or not as well-tested techniques, as long as the physician has a sufficient medical reason supporting that decision. Keeping accurate records and documentation backing up these decisions can greatly aid a physician attempting to defend a position based on the choice of one technique over another.

For the medical center, liability hinged on whether the surgeon was an employee or an independent contractor.The legal doctrine of *respondeat superior* allows an injured party to recover damages from an employer based on the actions of an employee, which typically gives the injured party a better chance for recovering actual damages. Physicians working for a hospital often are difficult to categorize due to the nature of their work. Courts can come out either way by holding physicians to be employees or independent contractors based on the particular circumstances of the relationship. Note also that some states prohibit hospitals from hiring physicians directly. This issue is a complicated and state-specific one tabled for present purposes, but it requires input from qualified legal counsel.

There are benefits and detriments to treating physicians as either one. A hospital has less control over an independent contractor physician, but it is less likely to be liable for the physician's actions. A hospital has more control over an employee physician, but it is more likely to be liable for the physician's actions. This decision is a difficult one to make, as thereare many implications, and it should be discussed with a competent attorney as the ramifications go beyond the medical practice realm and into tax considerations as well. Whichever route the hospital chooses to go, it is also important to work with competent counsel to craft appropriate documents to protect the hospital's legal position on that question should litigation subsequently ensue. In this case, the surgeon was found to be an employee of the medical center, which meant that the medical center could be held responsible for the total amount of the verdict.

## REFERENCE

DeKalb County Court, GA. Case No. 12A43890. June 23, 2014. ■