HEALTHCARE RISK MANAGEMENT™

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

INSIDE

Enclosed in this issue:

HIPAA Regulatory Alert: Cloud-based storage and document-sharing services

Legal Review & Commentary: $21.5 million verdict for locked-in syndrome; liability for misplaced tracheostomy

AHC Media

NOVEMBER 2015 Vol. 37, No. 11; p. 121-132

Crack down on OR antics as public, plaintiffs' bar learn of poor behavior

Imagine walking through a unit and seeing doctors and staff openly insulting patients, laughing at racist and misogynist remarks, and even making inappropriate sexual contact. Any risk manager would react with fury and realize that something was seriously wrong with the hospital culture and that it was creating all sorts of liability risks.

That behavior would never happen on an open unit. But is it happening in your operating rooms? Recent cases in the news have put a spotlight on disrespectful and even abusive behavior during surgery, and those cases might lead to closer scrutiny by patients, plaintiffs' attorneys, and regulators. That expected scrutiny means now is the time for risk managers to step in and put a halt to the antics that are common in some ORs.

"... COMPLAINING ... OR INSULTING THE PATIENT WHILE HE'S LYING UNCONSCIOUS IN FRONT OF YOU IS NOT AN OPTION." — JOHN BANJA, PHD, EMORY UNIVERSITY

A recent jury verdict brought attention to the issue. A Fairfax, VA, jury ordered an anesthesiologist and her practice to pay a patient $500,000 for disparaging remarks made during surgery and for entering a false diagnosis on his chart. The patient had left his smartphone recording when it was placed in the bag of patient belongings under the OR table. The case received extensive publicity, and it informed members of the public about what sometimes happens when they are unconscious. *(For more on that case, see* Healthcare Risk Management, *August 2015.)*

Soon after that secret was revealed, an essay in the *Annals of Internal Medicine* also brought attention to disrespectful behavior while patients

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. Arnold Mackles, MD, MBA, LHRM, physician reviewer, discloses that he is an author and advisory board member for The Sullivan Group and that he is owner, stockholder, presenter, author, and consultant for Innovative Healthcare Compliance Group.

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. customer.service@AHCMedia.com. AHCMedia.com

SUBSCRIPTION PRICES: USA, Print: 1 year (12 issues) with free CE nursing contact hours and free *AMA PRA Category 1 Credits*™, $519. Add $19.99 for shipping & handling. Online only, single user: 1 year with free CE nursing contact hours and free AMA PRA Category 1 Credits™, $469. Outside USA, add $30 per year, total prepaid in USA funds.

MULTIPLE COPIES: Discounts are available for group subscriptions, multiple copies, site-licenses or electronic distribution. For pricing information, call Tria Kreutzer at (866) 213-0844.

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.)

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 1.5 nursing contact hours using a 60-minute contact hour. Provider approved by the California Board of Registered Nursing, Provider #CEP14749, for 1.5 Contact Hours.

AHC Media designates this enduring material for a maximum of 1.5 *AMA PRA Category 1 Credits*™. Physicians should claim only credit commensurate with the extent of their participation in an activity.

Healthcare Risk Management™ is intended for risk managers, healthcare administrators, healthcare legal counsel, and physicians. This activity is valid 24 months from the date of publication.

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.

were anesthetized, including sexual innuendo and inappropriate touching. The essay was written by a physician, and the journal editors convinced him to remain anonymous. In an accompanying editorial, the editors called the incidents in the essay "disgusting and scandalous." They cited misogyny, disrespect, racism, and "heavy overtones of sexual assault." *(For more on that essay, see the story in this issue.)*

Though incidents of misbehavior might be rare in the context of all surgeries performed, any occurrence is "certainly too much and completely unprofessional," says **R. Stephen Trosty**, JD, MHA, ARM, CPHRM, president of Risk Management Consulting in Haslett, MI, and a past president of the American Society for Healthcare Risk Management (ASHRM) in Chicago. Trosty has dealt with serious OR misbehavior in the past when he was the risk manager at a hospital. *(For more on Trosty's experience with this issue, see the story in this issue.)*

Zero tolerance

Improper behavior has been a problem in ORs for years, but Trosty says the issue typically is addressed only when a particular incident comes to light or possibly in educational sessions directed at surgeons.

The issue also has been addressed by various medical boards, ethics and quality improvement committees at hospitals, and medical ethicists, with little success.

"Training and the telling of actual instances in which there have been lawsuits and judgments involving this type of behavior do not seem to have put a complete stop to it," Trosty says. "This type of behavior cannot and must not be tolerated by anyone. There usually are many medical professionals in an operating room, and none of them should accept this type of behavior." Given the common climate that the physician is the head of the operating room and the leader of the team, it might be difficult for staff members to say anything without feeling concern for their jobs, he says. "The hospital or other institution must establish a climate that makes it very clear that this type of behavior is unacceptable and will not be tolerated," Trosty says.

Environment is critical

Hospitals must create an environment in which people don't feel their jobs are in jeopardy if they speak up about this type of behavior.

That culture can be created and maintained only with the support of top administration and medical leadership, Trosty says. It is "unrealistic and naïve" for a risk manager to tackle this issue without

EXECUTIVE SUMMARY

A highly publicized lawsuit and public comments by healthcare leaders have made the public and the plaintiffs' bar more aware of the sometimes questionable behavior of OR personnel. Risk managers should prohibit unprofessional or disrespectful behavior during surgery.

- Creating the right culture is key to improving OR behavior.
- Misbehavior should be taken seriously, with appropriate repercussions.
- Don't assume that you know of all OR misbehavior.

support from the higher levels of authority, he says.

"The risk manager has to continue to have sessions about this, not only with physicians, but with all professionals who are in the operating room. They have to stress why this is completely unacceptable behavior that cannot be accepted or tolerated," Trosty says.

This education must be backed up by all levels of authority and responsibility within the organization, he emphasizes, or there will be a lack of compliance by those who are inclined to this type of behavior.

The training and risk management sessions by the risk managers should include examples and instances of actual occurrences and litigation, including the judgments against the participating physicians and/or other medical professionals, Trosty advises.

In addition, the risk management departments of insurance companies and medical societies might be resources for further educating physicians and staff. In addition to those groups reinforcing that this type of behavior will not be tolerated, physicians should be warned that their professional liability insurance can and usually will be cancelled if they are found guilty of this offense, Trosty notes.

"As long as this type of behavior is tolerated, if not accepted, within society, this type of behavior is likely to continue in those rare instances in which you have physicians and others who feel that they belong to the 'good old boys club' or that this type of behavior makes them appear to be part of the club," Trosty says. "We've seen that this actually can apply to female as well as male physicians."

The operating room has long been the one place in a hospital where administrators look the other way if personnel want to create their own atmosphere, whether that is quiet and professional or loud and irreverent, but that lack of response must change, 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 ASHRM. By its nature, the operating room always has been a challenge for oversight by risk managers, she notes.

Unlike other clinical areas, the risk manager cannot casually stroll through once in a while to observe behavior, she notes. Even if you go to the trouble of observing a procedure, the team members will be on their best behavior when the risk manager is present.

"A risk manager is never going to personally observe the kind of behavior that we're talking about," Kicklighter says. "That means the solution is in changing the culture, not trying to personally observe and intervene."

She suggests that risk managers make a concerted effort to be visible to the operating room staff by making periodic rounds to meet surgeons and OR staff members face to face, as well as holding inservices for the surgical team. That visibility will breed familiarity so that the risk manager doesn't stand out so much during a drop-in visit, and it also will encourage more trust when the risk manager advises members of the OR team on proper decorum.

"That also will help them so that when something improper happens in the operating room, they will feel comfortable in reporting it to the risk manager," Kicklighter says.

Enlightened patients

Patients are far more likely to become aware of misbehavior now with the proliferation of smartphones and other technology, notes **John Banja**, PhD, medical ethicist at the Center for Ethics at Emory University in Atlanta.

Banja recently was involved with a malpractice case in which a family recorded a conversation with a physician, and that recording turned out to be damning evidence that prompted a settlement.

Some types of inappropriate behavior, such as laughing at or ridiculing an anesthetized patient's body, are a matter of professionalism and respect for patients, Banja says, and that professionalism must flow from the hospital's culture. Angry or frustrated clinicians are somewhat different, he says. They must be told that while wanting to vent about patients and work is understandable, it is not the professional thing to do, he says.

"They are going to encounter patients who hit all their buttons and make them defensive or angry, and they're going to want to talk about it," Banja says. "Our job is to reassure them that that reaction is perfectly normal, but complaining about it or insulting the patient while he's lying unconscious in front of you is not an option. They will need to find other ways to deal with those frustrations."

SOURCES

- John Banja, PhD, Medical Ethicist, Center for Ethics, Emory University, Atlanta. Email: jbanja@emory.edu.
- Leilani Kicklighter, RN, ARM, MBA, CPHRM, LHRM, The Kicklighter Group, Tamarac, FL. Telephone: (954) 294-8821. Email: lkicklighter@kickrisk.net.
- R. Stephen Trosty, JD, MHA, CPHRM, President, Risk Management Consulting, Haslett, MI. Telephone: (517) 339-4972. Email: strosty@comcast.net. ■

Doctor reveals dirty secret about how operating room patients are treated

An essay in the *Annals of Internal Medicine* received the attention of not just the medical community, but also the general public, when it revealed how anesthetized patients are sometimes treated with disrespect and even subject to what could be considered assault.

Titled "Our Family Secrets," the physician author recounts incidents of misogyny, racism, and sexual assault in the operating room. In an accompanying editorial, the editors of the journal said that they debated whether to publish the sensational essay, but they said they did so to underscore that it's important that doctors not remain silent when they witness misconduct.

The author of the essay was teaching a medical humanities course to senior medical school students. During the course, he asked the students if any of them had something happen during their medical school experience that troubled them deeply.

One student expressed regret at not standing up to a surgeon's inappropriate behavior while a patient was under general anesthesia for a vaginal hysterectomy. While the surgeon was prepping the unconscious patient's vaginal area for the procedure, he looked at the student and said, "I bet she's enjoying this," accompanied with a laugh and wink.

The student called the surgeon a "dirtball" when recounting the incident, but expressed remorse that he had laughed along with the surgeon. He felt intimidated by the senior physician and didn't know what to do other than playing along with the joke.

The anonymous author also told his class of an incident that occurred when he was a third-year medical student. He had helped deliver a baby, but the mother experienced severe bleeding immediately after. The resident instructed the anesthesiologist to put the patient under and then proceeded with an internal bimanual uterine massage, which involves placing a hand inside the vagina and pressing a fist against the uterus to stop the blood flow.

Once the bleeding was controlled, the doctor said "Atta girl. That's what I like. A nice, tight uterus." Then he raised his free hand in the air and started singing "La Cucaracha," shuffling so it looked like he was dancing. (The patient was Latino). The essay author laughed and hummed along to the song until the anesthesiologist yelled at both of them to stop. *(Access to the essay is available online at http://tinyurl.com/oovn85m. The cost is $32.)* ■

Heads roll after OR team members invite others to laugh at patient

An incident involving an out-of-control OR team illustrates how undignified and abusive behavior can occur even at facilities with high standards.

R. Stephen Trosty, JD, MHA, ARM, CPHRM, president of Risk Management Consulting in Haslett, MI, and a past president of the American Society for Healthcare Risk Management (ASHRM) in Chicago, was a risk manager at a hospital when he learned of the incident.

A patient was about to undergo surgery, and when the OR staff undraped him, the man was found to have an extremely large penis and scrotum.

"Not only was this mentioned and laughed about by the people in the room, but other hospital personnel were invited to come into the operating room to witness this. It was referred to as a 'true gift of nature,'" Trosty recalls. "All sorts of comments were made about how fortunate his wife was and how talented he must be."

When Trosty learned of the incident from staff members who were bothered by it, he conducted an investigation to determine exactly what happened. Then he went to the chief of staff, the head of the department, the vice president of nursing, and the CEO to insist that it be dealt with immediately and effectively.

"Disciplinary action was taken at all levels, up to and including the firing of non-physician staff. The physician who was most responsible had his privileges revoked," Trosty says. "I am not sure that this actually permanently stopped the behavior, but I do believe it was a major deterrent to it happening again. All levels of the institution gave the

message that this type of behavior would not be tolerated, and it was explicitly stated that anyone who participated in this type of behavior in the future faced equally serious consequences."

The incident was used as a teaching example for staff and physicians thereafter. ■

Treat diagnosis errors as systemic, not individual human mistakes

[We posted a story about this report on Sept. 22 at AHCMedia.com. We emailed Healthcare Risk Management *subscribers to let them know that this story was posted. If you didn't receive the notice, then we don't have your email address. To receive notices about breaking news in the future, contact customer.service@AHCMedia.com.]*

Diagnostic errors are underappreciated and will require a collaborative approach to reduce them, according to a recent report from the Institute of Medicine (IOM).

IOM called on the healthcare community to address diagnosis errors by treating them as systemic problems and not human errors made by individuals. IOM's *Improving Diagnosis in Health Care* report outlines the steps necessary for reducing these errors. Although it has been estimated all Americans will suffer consequential diagnosis errors in their lifetimes, no reliable figures exist for how many occur each year, said **John R. Ball**, MD, JD, of Asheville, NC, chair of the Committee on Diagnostic Error in Health Care. The key report finding is that reducing diagnosis errors will require a collaborative effort among not just healthcare team members, but also the patient and family, he said. (*The IOM report is available online at http://tinyurl.com/oogmdas.)*

"The stereotype of a single physician contemplating a patient's presentation and discerning the diagnosis is not always true," Ball said. "The diagnostic process often involves intra- and inter-professional teamwork. Nor is diagnostic error always due to human error. It often occurs because of errors in the healthcare system."

The committee defines diagnostic error as "the failure to (a) establish an accurate and timely explanation of the patient's health problem(s) or (b) communicate that explanation to the patient." Despite the pervasiveness of diagnostic errors and the risk for serious patient harm, "diagnostic errors have been largely unappreciated within the quality and patient safety movements in healthcare," the report says. "Without a dedicated focus on improving diagnoses, these errors likely will worsen as the delivery of healthcare and the diagnostic process continue to increase in complexity."

The IOM report stops short of calling for mandatory reporting of diagnosis errors, but it emphasizes that healthcare providers must improve the entire diagnostic process, not just reduce errors. While acknowledging the pervasiveness of diagnostic errors, Ball warned against calls for mandatory public reporting.

"The committee believed that, given the lack of an agreement on what constitutes a diagnostic error, the paucity of hard data, and the lack of valid measurement approaches, the time was simply not ripe to call for mandatory reporting," Ball said. "Instead, it is appropriate at this time to leverage the intrinsic motivation of healthcare professionals to improve diagnostic performance and to treat diagnostic error as a key component of quality improvement efforts by healthcare organizations. Better identification, analysis, and implementation of approaches to improve diagnosis and reduce diagnostic error are needed throughout all settings of care."

Healthcare IT should be used more for diagnoses and not just billing or other administrative purposes, the report says. The report also calls for more involvement by radiologists and pathologists as members of the diagnostic team, and it praises the educational efforts of some medical malpractice insurers. The report comes nearly 16 years after IOM's landmark study *To Err*

EXECUTIVE SUMMARY

The Institute of Medicine has issued a report calling on the medical community to more effectively address diagnostic errors. Reducing these errors will require a collaborative approach.

- Diagnostic errors typically are not caused only by a physician's error.
- Radiologists and pathologists should be more involved with diagnoses.
- Risk managers should treat diagnostic errors as a system problem.

Is Human: Building a Safer Health System, which prompted a campaign to reduce medical errors.

The report outlines eight goals for improving diagnoses. *(See the story on those goals in this issue.)*

Problems related to diagnostic error are the most common allegation in medical malpractice claims, says Medical Director **David B. Troxel**, MD, of The Doctors Company, a malpractice insurance provider in Napa, CA.

"We agree with the recommendation in this new report that medical liability insurers collaborate with healthcare professionals on opportunities to improve diagnostic performance," Troxel says. He notes that The Doctors Company has the largest single database of diagnosis-related medical malpractice claims and shared claims data on diagnostic error with the IOM. The Doctors Company Foundation also provided funding for the report.

The report is a major milestone in the effort to improve diagnoses, quality of care, and patient outcomes, says **Mark Graber**, MD, founder and president of The Society to Improve Diagnosis in Medicine (SIDM), a member of the report committee.

"Diagnosis is one of the most difficult and complex tasks in healthcare. There are more than 10,000 potential diagnoses, thousands of lab tests, and the problem that symptoms of each diagnosis vary from person to person," he says. "Moreover, our healthcare systems are highly complex, which contributes to problems coordinating care and completing the diagnostic process successfully."

Diagnostic errors have no single root cause, says **Paul Epner**, executive vice president of SIDM and chair of the Coalition to Improve Diagnosis. SIDM recently spearheaded the launch of the Coalition to bring action to diagnostic errors.

"This report addresses a significant gap in our knowledge, and SIDM intends to drive review and action on the recommendations across the entire healthcare system. It is the responsibility of everyone involved in the diagnostic process to consider the steps they can take to improve outcomes," Epner says. "This begins with healthcare providers and their organizations, which need to establish a culture of safety where these errors can be identified, studied, and addressed."

SOURCE

- **David B. Troxel**, MD, Medical Director, The Doctors Company, Napa, CA. Email: dtroxel@thedoctors.com. ■

IOM cites 8 goals for reducing diagnosis errors

The Institute of Medicine's *Improving Diagnosis in Health Care* report outlines the following eight goals for reducing diagnosis errors:

• Facilitate more effective teamwork in the diagnostic process among healthcare professionals, patients, and their families. The diagnostic process hinges on successful collaboration among healthcare professionals, patients, and their families. Patients and their families are critical partners in the diagnostic process. In addition, all healthcare professionals need to be well-prepared and supported to engage in diagnostic teamwork.

• Enhance healthcare professional education and training in the diagnostic process. Getting the right diagnosis depends on all healthcare professionals involved in the diagnostic process receiving appropriate education and training. Improved emphasis on diagnostic competencies and feedback on diagnostic performance is needed.

• Ensure that health information technologies (IT) support patients and healthcare professionals in the diagnostic process. Although health IT has the potential to improve diagnosis and reduce diagnostic errors, many experts are concerned that it is not effectively facilitating the diagnostic process and might even be contributing to errors. Collaboration among health IT vendors, users, and the Office of the National Coordinator for Health Information Technology is needed to better align health IT with the diagnostic process.

• Develop and deploy approaches to identify, learn from, and reduce diagnostic errors and near misses in clinical practice. Few healthcare organizations have processes in place to identify diagnostic errors and near misses in clinical practice. However, collecting this information, learning from these experiences, and implementing changes are critical for achieving progress. Healthcare professional societies also can be engaged to identify high-priority areas to improve diagnosis.

• Establish a work system and culture that supports the diagnostic process and improvements in diagnostic performance. The work system and culture of many healthcare organizations could better support the diagnostic process. For example, healthcare organizations

should promote a non-punitive culture that values feedback on diagnostic performance, ensures effective communication in diagnostic testing, and designs a work system that supports team members involved in the diagnostic process, including integrating error recovery mechanisms.

• **Develop a reporting environment and medical liability system that facilitates improved diagnosis through learning from diagnostic errors and near misses.** There is a need for safe environments, without the threat of legal discovery or disciplinary action, in which diagnostic errors, near misses, and adverse events can be analyzed and learned from to improve diagnosis and prevent diagnostic errors. Voluntary reporting efforts should be encouraged and evaluated for their effectiveness. Reforms to the liability system are needed to make healthcare safer by encouraging transparency and disclosure of medical errors, including diagnostic errors.

• **Design a payment and care delivery environment that supports the diagnostic process.** Payment likely influences the diagnostic process and the occurrence of diagnostic errors. For example, fee-for-service payment lacks incentives to coordinate care, and distortions between procedure-oriented and cognitive-oriented care might be diverting attention from important tasks in the diagnostic process. A fundamental research need is an improved understanding of the impact of payment and care delivery models on diagnosis.

• **Provide dedicated funding for research on the diagnostic process and diagnostic errors.** Federal resources devoted to diagnostic research are overshadowed by those devoted to treatment. Dedicated, coordinated funding for research on diagnosis and diagnostic error is warranted. Public/private collaboration and coordination can help extend financial resources to address research areas of mutual interest. ■

EHR gag clauses could hamper evaluation and patient safety at healthcare facilities

There is a likelihood that the contract for the electronic health record (EHR) used at your hospital or health system includes a gag clause that prohibits talking to others about any dissatisfaction with the product. There are concerns that the gag clauses interfere with proper assessment of EHRs, which could in turn threaten patient safety.

An investigation by the web site Politico found that many contracts for EHRs include "gag clauses" that effectively forbid healthcare providers from talking about problems of dissatisfaction with the software. Politico obtained 11 contracts from hospitals and health systems in New York City, California, and Florida, all of them using EHRs from six of the biggest vendors. With one exception, every contract contains a gag clause.

"This is the first time the existence of the EHR gag clauses has been conclusively documented," according to Politico. *(For the original report on that investigation, go to http://tinyurl.com/naeryo6.)*

The gag clauses became standard in EHR contracts when the technology was new and have remained since then, says **Gary S. Sastow**, JD, a partner with Brown, Gruttadaro, Gaujean and Prato in White Plains, NY. He believes that the gag clause issue came into being due to physicians generally being opposed to EHR implementation. The theory behind the clauses was that criticism might have been unfairly placed with the software when, in reality, the criticism was directed at the overall concept.

Now that the medical community has moved beyond that point and physicians have accepted the reality of using EHR systems, Sastow believes criticism might now be more fair and says gag clauses are not appropriate. Users should be free to discuss their systems openly and honestly and

EXECUTIVE SUMMARY

Most electronic health record (EHR) contracts include gag clauses that prohibit physicians and others from talking about shortcomings. These restrictions could threaten patient safety if users are reluctant to report problems.

- A recent investigation found that almost all EHR contracts include gag clauses.
- Hospitals should resist gag clauses whenever possible.
- The clauses can be enforced.

share "the good, the bad, and the ugly," he says.

Importantly, a gag clause should not prohibit internal criticism of an EHR, Sastow says. They prohibit criticizing the EHR to outside parties, but not within the organization, he explains. The real danger from the gag clauses is that physicians and staff might be intimidated, overly cautious, and reluctant to discuss any EHR problems even within the organization.

"The intent of the gag clauses is to keep one hospital from calling another and saying, 'Here's our experience,' or 'Don't go with this company because we're having all these problems,'" Sastow says. "That's how people do business, and there's a lot of value in hearing about someone else's experience. But with these gag clauses, the manufacturer is blocking that."

The gag clauses can be enforced, he says, but Sastow knows of no litigation accusing a hospital for violating the clause. He says hospitals should try to have the gag clauses removed from the contracts by using the argument that if the company is confident in their product, there should be nothing bad to say. The issue is worth fighting over because EHR vendors could decide at any point to enforce the gag clauses, he says.

"If the clause can't be removed, at least negotiate carve-outs that would make it much more difficult to prove a breach of contract," Sastow advises. "The carve-out could say that if there already is information in the public about this software and its weaknesses, then you can talk about it too, and there is no violation. When the information is no longer confidential, you should be able to put your two cents in because you're not divulging anything confidential."

Gag clauses could come into play with an EHR problem that is becoming increasingly common in malpractice litigation, says attorney **R. Douglas Vaughn**, JD, chair of the Medical Defense and Health Law Committee of the International Association of Defense Counsel (http://www.iadclaw.org) and a partner with Deutsch, Kerrigan & Stiles in Gulfport, MS. Attorneys are reporting difficulty in obtaining complete copies of a patient's record because sometimes the same EHR system produces different versions every time it is requested, he says.

Incomplete and inconsistent records can hinder the hospital or physician's defense, but Vaughn says the gag clauses prohibit them from reporting those problems in a survey or other communication within the medical community. Similarly, there have been reports of EHR errors in which patient records were comingled, which resulted in patients receiving the wrong medication or treatment, he says.

"Those are the kinds of bugs you want to report and warn others about, but these gag clauses can keep you from doing that," Vaughn says. "A lesson for the hospital is that you have to keep all this in mind when you're considering the pros and cons of an EHR, because you may not be aware of what everyone else thinks of it. "

SOURCE

- **Gary S. Sastow**, JD, Partner, Brown, Gruttadaro, Gaujean and Prato, White Plains, NY. Email: gsastow@bggplaw.com. ■

Health system is thought to be first to provide universal suicide screenings

In what appears to be a first for a health system, Parkland Health & Hospital System in Dallas recently implemented suicide screenings for all patients.

The program is the first of its type in the United States, according to **Kimberly Roaten**, PhD, director of quality for safety, education, and implementation in the Department of Psychiatry at Parkland and associate professor of psychiatry at The University of Texas Southwestern Medical Center, also in Dallas. A clinical psychologist working with Parkland patients, Roaten is one of the leaders who developed the new program.

"The Joint Commission requires healthcare providers screen all patients with psychological problems for suicide risk," Roaten notes. "But we believe it's important to screen everyone because some of this risk may go undetected in a patient who presents for treatment of non-psychiatric symptoms."

In 2014 Parkland dedicated the resources needed to make this possible. Those resources included hiring 12 psychiatric social workers, selecting a standardized and validated suicide screening instrument, building an algorithm in the electronic health record that triggers the appropriate clinical intervention depending on the patient's answers to a few simple questions, and training all nursing staff to implement the program.

Parkland implemented suicide risk screening with all emergency department patients and hospital

inpatients in February 2015, says **Celeste Johnson**, DNP, APRN, PMH CNS, director of nursing in psychiatric services at Parkland.

"In late May, we transitioned from the previous screening program to the standardized suicide risk screening at all Parkland community-oriented primary care health centers and also at the correctional health division for all inmates at the Dallas County Jail," Johnson says. "Our goal is to screen every patient using proven screening tools that can help us save lives."

Parkland has screened more than 100,000 patient encounters at the hospital and emergency department, and it has screened more than 50,000 patient visits in outpatient settings. Parkland uses the Columbia Suicide Severity Rating Scale (C-SSRS), a validated screening tool developed by Columbia University in New York City, with adults 18 and older and the ASQ (Ask Suicide Screening Questionnaire), developed by the National Institute of Mental Health in Bethesda, MD, with 12- to17-year-olds.

The Parkland algorithm sorts patients into three suicide risk categories based on their answers to the screening questions: no risk identified, moderate risk identified, and high risk identified. Those at high risk are immediately placed under one-to-one supervision, suicide precautions are implemented, and an evaluation by a behavioral health clinician is initiated. Patients at moderate risk are automatically referred to a psychiatric social worker and usually are seen during the same visit. If patients choose not to speak with a psychiatric social worker during the visit, they will receive a follow-up phone call to provide additional support and resources.

For example, a patient might come in with a sprained ankle or sore throat, but if his or her suicide risk screening shows moderate risk, Parkland's clinical algorithm immediately alerts a member of the behavioral health team to come and speak with the patient. Before discharge, moderate- and high-risk patients also are given information about suicide warning signs, suicide crisis center hotline numbers, and Dallas County community mental health resources.

So far, the suicide risk screening in the emergency department and inpatient units at Parkland has found 1.8% of patients to be at high risk and approximately 4% at moderate risk for suicide.

"To our knowledge we are the first big hospital system in the U.S. to implement a universal screening program for suicide risk, and the data we are gathering will be significant for other organizations in the future," Roaten says. ■

Hospital cited for exposing staff to patient violence

Federal officials recently cited Bergen Regional Medical Center in Paramus, NJ, for failing to protect employees from violent patients.

Responding to an employee complaint, the Occupational Safety and Health Administration (OSHA) found eight incidents from Feb. 22 through June 12 in which healthcare workers were victims of violent patients, including one incident in which a nurse suffered a laceration and bruises attempting to stop an attack on a patient.

Bergen Regional Medical Center is one of the nation's largest hospitals, providing long-term, behavioral health, and acute care in northern New Jersey. It has more than 1,070 beds, and it is also one of the state's largest licensed nursing homes.

OSHA cited the facility for one general duty clause citation for failing to keep the workplace free of hazards. Employees reported incidents that involved patients barricading workers in a room, threatening them, and exposing them to bloodborne pathogens. Several employees experienced being bit, punched, kicked, and threatened by patients, according to a statement released by **Lisa Levy**, director of OSHA's Hasbrouck Heights Area Office. *(More information on the OSHA citation is available online at http://tinyurl.com/owjq2s6.)*

"Bergen Regional Medical Center's management recognized workplace hazards, but lacked adequate procedures to prevent employee exposure," Levy says. "With so many incidents, it's clear that this facility's workplace violence program is ineffective and should be improved immediately to protect employees and ensure a safe workplace."

OSHA issued one repeated citation for incorrectly recording workplace injuries on the OSHA 300A illness and injury reporting form. Proposed penalties total $13,600.

In June, the agency expanded use of its enforcement resources in hospitals and nursing homes to focus on workplace violence, one of the most common causes of injuries among healthcare workers. Guidelines for preventing workplace violence for health and social service workers are available at http://tinyurl.com/ohwgnoe. ■

Adventist to pay $115M to settle fraud claims

Adventist Health System, based in Altamonte Springs, FL, has agreed to pay the United States $115 million to settle allegations that it violated the False Claims Act by maintaining improper compensation arrangements with referring physicians and by miscoding claims, the Justice Department announced recently.

Adventist is a non-profit healthcare organization that operates hospitals and other healthcare facilities in 10 states.

Principal Deputy Assistant Attorney General **Benjamin C. Mizer**, JD, head of the Justice Department's Civil Division, announced the settlement. "Unlawful financial arrangements between heathcare providers and their referral sources raise concerns about physician independence and objectivity," Mizer said. "Patients are entitled to be sure that the care they receive is based on their actual medical needs rather than the financial interests of their physician."

The settlement resolves allegations that Adventist submitted false claims to the Medicare and Medicaid programs for services rendered to patients referred by employed physicians who received bonuses based on a formula that improperly took into account the value of the physicians' referrals to Adventist hospitals. Adventist-owned hospitals allegedly paid doctors' bonuses based on the number of tests and procedures they ordered, said Acting U.S. Attorney **Jill Westmoreland Rose**, JD, of the Western District of North Carolina.

"This type of financial incentive is not only prohibited by law, but can undermine patients' medical care. Would-be violators should take notice that my office will use the False Claims Act to prevent and pursue health care providers that threaten the integrity of our health care system and waste taxpayer dollars."

The settlement also resolves allegations that Adventist submitted bills to Medicare for its employed physicians' professional services containing certain improper coding modifiers, and thereby obtained greater reimbursement for these services than entitled.

The allegations arose from two

United States Postal Service

Statement of Ownership, Management, and Circulation

1. Publication Title	2. Publication Number	3. Filing Date
Healthcare Risk Management	1 0 8 1 – 6 5 3 4	10/1/15
4. Issue Frequency	5. Number of Issues Published Annually	6. Annual Subscription Price
Monthly	12	$519.00

7. Complete Mailing Address of Known Office of Publication *(Not printer) (Street, city, county, state, and ZIP+4)*
950 East Paces Ferry Road NE, Ste 2850, Atlanta
Fulton County, GA 30326-1180

Contact Person: Peter Balch
Telephone: 404-262-5434

8. Complete Mailing Address of Headquarters or General Business Office of Publisher *(Not printer)*
950 East Paces Ferry Road NE, Ste 2850, Atlanta, GA 30326-1180

9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor *(Do not leave blank)*

Publisher *(Name and complete mailing address)*
AHC Media LLC, David Fournier, President and CEO
950 East Paces Ferry Road NE, Ste 2850, Atlanta, GA 30326-1180

Editor *(Name and complete mailing address)*
Joy Dickinson, same as above

Managing Editor *(Name and complete mailing address)*
same as above

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

Full Name	Complete Mailing Address
AHC Media LLC	950 East Paces Ferry Road NE, Ste 2850, Atlanta, GA 30326-1180
David Fournier	950 East Paces Ferry Road NE, Ste 2850, Atlanta, GA 30326-1180
~~Bethany Schilling~~	~~950 East Paces Ferry Road NE, Ste 2850, Atlanta, GA 30326-1180~~
~~Lone Peak Capital Group, LLC~~	~~79 West Paces Ferry Road, Suite 200-A, Atlanta, GA 30305~~

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

Full Name	Complete Mailing Address

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

PS Form **3526,** October 1999 *(See Instructions on Reverse)*

COMING IN FUTURE MONTHS

- Should you disclose errors to pediatric patients?
- Liability risks of 3D printing
- How to respond to a patient's fake identification
- Do EMRs monopolize nurses' time?

lawsuits that were filed respectively by whistleblowers who worked at an Adventist hospital in Hendersonville, NC, and another whistleblower who worked at the corporate office of Adventist, under the *qui tam* provisions of the False Claims Act. The act permits private parties to file suit on behalf of the United States for false claims and to share in any recovery. The whistleblowers' share of the settlement has not yet been determined.

More information on the settlement is available online at http://tinyurl.com/pfb2bct. ■

13. Publication Title Healthcare Risk Management			14. Issue Date for Circulation Data Below September 2015	
15. Extent and Nature of Circulation			Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Total Number of Copies *(Net press run)*			334	307
b. Paid and/or Requested Circulation	(1)	Paid/Requested Outside-County Mail Subscriptions Stated on Form 3541. *(Include advertiser's proof and exchange copies)*	275	254
	(2)	Paid In-County Subscriptions Stated on Form 3541 *(Include advertiser's proof and exchange copies)*	0	0
	(3)	Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Non-USPS Paid Distribution	4	3
	(4)	Other Classes Mailed Through the USPS	23	18
c. Total Paid and/or Requested Circulation *[Sum of 15b. (1), (2),(3),and (4)]* ▶			302	275
d. Free Distribution by Mail *(Samples, complimentary, and other free)*	(1)	Outside-County as Stated on Form 3541	12	12
	(2)	In-County as Stated on Form 3541	0	0
	(3)	Other Classes Mailed Through the USPS	0	0
e. Free Distribution Outside the Mail *(Carriers or other means)*			5	5
f. Total Free Distribution *(Sum of 15d. and 15e.)* ▶			17	17
g. Total Distribution *(Sum of 15c. and 15f)* ▶			319	292
h. Copies not Distributed			15	15
i. Total *(Sum of 15g. and h.)* ▶			334	307
j. Percent Paid and/or Requested Circulation *(15c. divided by 15g. times 100)*			95%	94%

16. Publication of Statement of Ownership
☑ Publication required. Will be printed in the November 2015 issue of this publication. ☐ Publication not required.

17. Signature and Title of Editor, Publisher, Business Manager, or Owner
David R. Fournier Publisher & CEO — Date 09/10/2015

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

Instructions to Publishers

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

Failure to file or publish a statement of ownership may lead to suspension of Periodicals authorization.

PS Form **3526,** October 1999 *(Reverse)*

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.

NIST guide aims to make EHRs safer

The National Institute of Standards and Technology (NIST) has released a new guide that addresses a common concern with electronic health records: If they're not user-friendly, the potential benefits might never be recognized, and they could even threaten patient safety.

The guide states that safety improves when an electronic health record is made more usable. NIST researchers used five methods of data collection. They found three significant problems stemming from electronic health record use that led to suboptimal and unsafe patient care.

These were the problems they identified:

- problems with identification, consistency, and integrity of the information, such as inability to retrieve information from the record;
- lost data;
- information in multiple locations.

The researchers also identified other common problems with electronic health record use, including unintended actions, the likelihood of use errors, and a "high level" of user frustration.

NIST defines usability as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use." Usability represents an important, yet often overlooked, factor impacting the adoption and meaningful use of electronic health records, the report says.

The NIST report is available online at http://tinyurl.com/px5crzz. ■

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 AHCMedia.com site to take a post-test. Go to "My Account" to view your available CE activities. First-time users will have to register on the site using the 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.

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/CME QUESTIONS

1. **According to R. Stephen Trosty, JD, MHA, ARM, CPHRM, president of Risk Management Consulting, what should be included in the training and risk management sessions by the risk managers regarding proper OR behavior?**

   A. Examples and instances of actual occurrences and litigation, including the judgments against the participating physicians and/or other medical professionals
   B. Only the standards and guidelines established by professional organizations

2. **What does Leilani Kicklighter, RN, ARM, MBA, CPHRM, LHRM, a patient safety and risk management consultant with The Kicklighter Group, recommend as a way to improve OR behavior?**

   A. Leave the matter to the OR manager, because he or she will resent a risk manager's involvement.
   B. Bring in a consultant to study the current behavior in the OR and make recommendations.
   C. Appoint one nurse in the department to report observations directly to risk management.
   D. The risk manager should visit the department often and become better acquainted with physicians and staff.

3. **What is one of the Institute of Medicine's goals for reducing diagnostic errors?**

   A. Ensure that health information technologies support patients and healthcare professionals in the diagnostic process.
   B. Focus more resources on identifying individuals responsible for errors.
   C. Reduce the number of clinicians involved in making a diagnosis.

4. **According to Gary S. Sastow, JD, a partner with the law firm of Brown, Gruttadaro, Gaujean and Prato, which of the following is true of the gag clauses found in most EHR contracts?**

   A. They are not enforceable.
   B. They prohibit criticizing the EHR within the organization, but not to outside parties.
   C. They prohibit criticizing the EHR to outside parties, but not within the organization.

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Healthcare providers must closely examine cloud-based storage and document-sharing services

Are you using an Internet-based storage document-sharing application with protected health information (PHI)? If so, you might not have properly assessed the security of that application, and that missed step, alone, could be deemed a HIPAA violation.

That's the lesson from a recent settlement involving a hospital that used an Internet-based document-sharing application without having analyzed the risks associated with such a practice, says **Nathan A. Kottkamp**, JD, a partner with McGuireWoods in Richmond, VA. The Department of Health and Human Services Office for Civil Rights (OCR) recently announced a settlement with St. Elizabeth's Medical Center (SEMC) in Brighton, MA. The hospital agreed to pay $218,400 in fines and abide by a lengthy corrective action plan.

OCR Director **Jocelyn Samuels** issued a statement warning that organizations "must pay particular attention to HIPAA's requirements when using internet-based document-sharing applications."

Essentially, the issue in the SEMC case was that the hospital didn't treat the cloud provider as a business associate, Kottkamp explains. OCR investigated following a complaint about the use of the document-sharing app. OCR also was notified of a separate PHI breach related to data stored on a former workforce member's unsecured personal laptop and USB flash drive. These violations compromised 1,093 individuals' PHI, OCR reported.

In addition to the fine, the hospital agreed to assess and revise policies and procedures related to electronic storage and transmission of PHI. SEMC must submit proposed revisions to HHS for review and approval. In addition, SEMC has agreed to promptly investigate all "reportable events," or instances in which a workforce member has failed to comply with data privacy policies, Kottkamp explains. All reportable events must be submitted immediately to HHS for review and after one year, SEMC also must submit a summary of all reportable events, along with actions taken to mitigate harm and prevent recurrence. The hospital also must submit an attestation that all workforce members have completed all required training relating to PHI.

Closer look at e-storage

Kottkamp says the SEMC settlement is another example of increased emphasis that OCR is placing on security of PHI stored and transmitted electronically.

"It's becoming more and more prevalent to use cloud services of one sort or another, and many times we don't think much of it. There's an app to use, and there goes the document," he says. "The definition of business associate, we have to presume, includes cloud storage providers, because OCR says that anyone who maintains PHI is considered a business associate even if they don't necessarily have direct access to it."

OCR has promised in the past to address the question more directly, but it has not offered guidance yet. Including these apps in the business associate definition might not be appropriate, because many of them have no knowledge of what information is in the stored documents and cannot access it, Kottkamp suggests. Nonetheless, OCR has said in the past that they must be business associates because if there is a breach, the storage provider is obligated under the notification rules.

"It's a real challenge because providers don't necessarily think to engage cloud hosts as business associates, and most of the cloud providers are not capable of fulfilling their requirements as a business associate, regardless of whether they'd be willing to sign a business associate agreement in

EXECUTIVE SUMMARY

Cloud-based applications for the storage and exchange of documents must have adequate security and HIPAA compliance before using them for protected health information (PHI). Failure to examine the service can result in a HIPAA violation even if no PHI is compromised.

- Conduct your own assessment of a vendor's security and compliance.
- Insist on a third-party validation also.
- Prohibit employees from signing up directly with cloud vendors.

the first place," Kottkamp says.

Even if the cloud provider acknowledges being a business associate, it might not be willing to sign a healthcare organization's business associate agreement (BAA) because the obligations and risk are not worth the business potential, he notes. "If you're a hospital and have specific terms in your BAA, good luck trying to get Google to sign that before you use Google Docs," Kottkamp says. "Google is just not going to do that."

Some cloud providers might promote themselves as HIPAA-compliant and be willing to sign BAAs, Kottkamp says. However, he also cautions about vendors who seem too eager to sign your BAA. "If they are just so eager to sign the agreement and don't ask you anything at all about it, you might wonder if they're just signing it to close the deal, but compliance is nonexistent," he says. "Vetting of vendors is an obligation of healthcare providers these days."

When properly vetted to ensure security and HIPAA compliance, working with only one cloud storage provider could even improve PHI security for the hospital, Kottkamp says. Using one reliable cloud provider could reduce the risk of having documents stored on individual laptops and jump drives, the sources of many HIPAA breaches.

Hospitals should conduct a vendor risk assessment before signing a BAA with a cloud storage provider, says **Dan Zitting**, CPA, CISA, GRCA, vice president of product design and management at ACL Services, based in Vancouver, Canada. ACL Services provides risk management and audit services, including some cloud-based services, to healthcare organizations. He previously worked as an IT security auditor for hospitals.

"You want to understand the vendor's approach to security control and make sure they have mapped out everything related to HIPAA security and privacy," he says. "HIPAA is more difficult in this regard than some other compliance concerns because there is no actual certification for vendors."

A hospital also should insist on a third-party audit or validation of the vendor's data security and HIPAA compliance, Zitting says. Though there is no HIPAA certification, many other certifications include the same data security that is of concern with HIPAA. The ISO-9000 certification from the International Organization for Standards (ISO) is one example.

Kottkamp also cautions that a hospital can find its PHI on a cloud storage system without any of this happening if an employee bypasses the IT department. This situation can happen if the employee wants to use a cloud storage system for convenience, even thinking it offers better security, and arranges the service directly.

"It doesn't go through the normal vendor risk management process. We see that happening all the time," Kottkamp explains. "There have to be policies and procedures about how PHI is stored and transmitted, particularly when using a cloud-based service outside the hospital, emphasizing that the hospital must approve the vendor first. I don't think very many hospitals have written that policy or made it extremely clear to employees." ■

Do this immediately when you learn of a violation

You're sitting at your desk, and someone walks in to inform you that there has been a HIPAA violation. What do you do next?

The answer to that question could have significant impact on the scope of the violation and the resulting penalties and other costs. An alleged or actual HIPAA breach can result in catastrophic consequences, including not only costly investigative, analysis, reporting, and mitigating actions, but potentially costly fines and penalties, loss of patients, loss of personnel involved in the breach, and reputational harm, notes **Lani Dornfeld**, JD, a member in the health law practice at the law firm of Brach Eichler in Roseland, NJ.

Preparing for this moment is key to handling it well, notes **Fred Charlot**, director of Berkeley Research Group in Houston, TX, which provides consulting for healthcare and other organizations. That preparation means creating an incident response plan that spells

out in detail what you will do after learning of a breach, including the names and contact information for everyone who will be notified or participate in the investigation.

"Failure to have a response plan in place is really bad," Charlot explains. "Then you're making decisions and trying to remember things as you're troubled and trying to deal with the incident as it's occurring. You have a really good chance of missing something in that situation."

The incident response plan should include managerial items such as a reporting chain, whom to call, what order to call, and what actions to take. The plan should call for contacting not just IT, but also legal counsel, financial managers, public relations, and senior management.

Of course, the hospital must notify HHS and follow the rest of the breach notification rules, though that will not be the first action item. For information on how to report the breach to HHS, go to http://tinyurl.com/yap3lpb.

Shut off flow of PHI

Dornfeld agrees that planning ahead is crucial, and she adds that a response plan will allow you to act more quickly and effectively.

"The first step is putting the privacy officer and, where appropriate, the security officer, into action and, where needed for larger breaches, assembling a response team to manage the process," Dornfeld says.

The response team might include the privacy and security officers, a compliance committee, and other relevant hospital officials. If cloaking the investigation in the attorney-client privilege will be beneficial to the hospital, legal counsel should be engaged as soon as possible, Dornfeld notes.

EXECUTIVE SUMMARY

What you do immediately after a HIPAA violation can affect the severity and eventual penalties. Prepare a response plan before a breach occurs.

- Priorities should be notifying others in the hospital and establishing an investigative team.
- You have to stop the flow of protected health information immediately.
- Coordinate with external contacts such as insurers.

A key concern is stopping the breach, but Charlot says your first priority should be shutting off the flow of PHI and not necessarily ending the breach entirely if it involves a cyberattack from outside. In those cases, IT investigators will need to examine how the breach happened and what the attackers were after, and that can be more difficult if you slam the doors right away.

Because the breach investigation is the cornerstone of all actions to follow, the investigation must be undertaken and executed in a careful and planned manner, Dornfeld says. Everyone involved in the incident should be interviewed.

"My experience is that two interviewers to one interviewee, in a private area, is best. Careful and detailed notes must be taken of all interviews, including date and time," Dornfeld says.

Other actions should be undertaken in tandem, she advises. If the breach involved electronic information, you must initiate a forensic investigation to determine the root cause, and you must implement mitigating actions to contain the breach or the root cause of the breach. Document all actions carefully.

Depending upon what you find out from your initial investigation, in some situations it might be prudent to talk to the subject of the breach: the patient, Dornfeld says. This action is especially the case if the individual who is the subject of the breach is the one who brought the incident to the attention of the hospital. In that case, the hospital should conduct an interview of the individual to elicit information or evidence that the patient might have about how the breach happened.

"This is also a good time to ask questions that may uncover the truthfulness or accuracy of allegations," Dornfeld says. "However, the hospital should avoid providing too much information too early. Such conversations should include assurances that the hospital takes the privacy and security of patient information seriously and that it has initiated an investigation into the matter, has taken mitigating actions, if applicable, and will provide further information when available."

The hospital should avoid making promises that it will fire those involved, even if the patient is requesting that action, Dornfeld says. "Diplomacy and apology at this stage is generally best," she says.

Once all investigative actions have concluded, the response team should perform a risk analysis as required under HIPAA to determine whether there is more than a low risk that the PHI of the individual was compromised. If the answer is yes, the hospital must provide written notification of the breach.

Depending on the size and scope of the breach, the hospital might want to hire public relations professionals

to help reduce the potential for reputational harm, Dornfeld suggests. All actions taken will need to be set forth in a written report the hospital retains in its files, she adds.

Your response plan should include coordinating with any outside parties that should be involved, notes **Beth Strapp**, health care customer segment manager and vice president, Chubb Specialty Insurance, Simsbury, CT. That coordination could include insurers, particularly if the hospital has coverage for cyber or network security.

"Most insurers these days have some sort of a breach coach as part of the insurance policy," she says. "The breach coach acts as the quarterback, helping you analyze all aspects of breach and determine things like whether it violated additional state laws or federal regulations. If they think you need more help from forensics experts, for instance, they can bring that in, as well."

Strapp notes that a breach cannot be handled optimally unless it is reported promptly to the right people. If an employee detects a breach but doesn't report it properly, valuable time can be lost. "There's a huge responsibility on the organization to make sure you are training employees to know who they are supposed to contact and the importance of doing so quickly, so the organization can, in turn, respond appropriately," Strapp says.

After the initial response and investigation, follow-up actions by the oganization might include security risk analyses, technological changes to increase protections, changes in protocols for handling patient information, staff education, and staff discipline.

Dornfeld says, "Ultimately, every breach, small or large, should be used as an opportunity to remind all hospital personnel of the importance of protecting patient information and following proper privacy and security protocols." ■

Healthcare by far top target for cyberattacks

The healthcare industry sees 340% more security incidents and attacks than the average industry, according to a recent report.

The Raytheon/Websense Security Labs' *2015 Industry Drill-Down Report — Healthcare* notes that medical information is 10 times more valuable than other types of information on the black market, which makes healthcare a major target for cybercriminals. The proliferation of electronic health records creates a data-heavy environment, while networks comprising thousands of providers present an enormous attack surface, the report says.

"The rapid digitization of the healthcare industry, when combined with the value of the data at hand, has led to a massive increase in the number of targeted attacks against the sector," said **Carl Leonard**, Raytheon/Websense principal security analyst, in a statement accompanying the report. "While the finance and retail sectors have long honed their cyber defenses, our research illustrates that healthcare organizations must quickly advance their security posture to meet the challenges inherent in the digital economy — before it becomes the primary source of stolen personal information."

In 2014, Websense identified a 600% increase in cyberattacks against hospitals within a 10-month period. As a follow up to this discovery, Raytheon/Websense Security Labs recently examined the real-world attack telemetry against healthcare, and it uncovered new intelligence about the most prolific and effective cyberattack tools, techniques, and security trends impacting the industry.

One in every 600 attacks in the healthcare sector involve advanced malware, according to the report. In fact, the healthcare sector is four times more likely to be impacted by advanced malware than any other industry. "With many organizations lacking budget and the administrative, technical or organizational skills necessary to detect, mitigate and prevent cyber-attacks, advanced malware presents a significant threat to healthcare infrastructure," the report says.

Additionally, the healthcare sector is 74% more likely to be impacted by phishing schemes. A lack of effective security awareness training and employee security awareness programs often compounds the danger of increased phishing attempts, which results in more security incidents, the report notes.

Healthcare is 4.5 times more likely to be impacted by the malware Cryptowall and three times more likely to be impacted by the malware Dyre. Dyre was first used to target the financial sector and successfully stole hundreds of millions of dollars. New exploit capabilities make Dyre malware a significant data loss threat for healthcare organizations worldwide, the report explains, while Cryptowall encrypts and holds hostage critical healthcare data for ransom. *(The full report is available at http://tinyurl.com/phk339s.)* ■

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

Hospital loses $21.5 million claim against veteran suffering from locked-in syndrome

By ***Damian D. Capozzola****, Esq.*
The 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

David Vassalli*, 2016 JD Candidate*
Pepperdine University School of Law
Malibu, CA

News: In October 2010, a Navy veteran went to a veterans hospital complaining of a headache and loss of peripheral vision. The man was seen by several physicians, and a CT scan was ordered. The CT scan revealed that the man suffered from an ischemic stroke, which is characterized as a stroke that occurs due to the blood supply to the brain being cut off. Eventually the source of the man's minor stroke was determined to be cardioembolic, meaning it originated in his heart, but initially physicians were unsure where the stroke occurred. Without completing the practice referred to as "secondary stroke prevention," which entails numerous steps designed to reduce a second stroke, the man was released and given baby aspirin to reduce the likelihood of a second stroke.

Just more than five weeks later, the man suffered a second stroke that resulted in locked-in syndrome. The man is now a quadriplegic who has fully functioning cognitive abilities but can move only his eyes and his head in a limited manner.

The man brought a claim against the doctors at the veterans hospital for failing to take the proper steps to prevent the second stroke. The defense argued that baby aspirin was the proper treatment and that treatment with warfarin would have been impossible because the man was being stubborn and uncooperative. The judge agreed with the man and found the doctors committed medical malpractice by failing to take more steps to prevent the second stroke. As such, the judge awarded the man $21.5 million.

Background: On Oct. 21, 2010, a 56-year-old Navy veteran was experiencing a headache and loss of vision. The man entered a veterans hospital seeking treatment. He was seen by numerous physicians, one of whom was an optometrist who ran a test for the man's loss of vision. The optometrist determined that the man was experiencing incongruous right homonymous hemianopia, which is typically associated with a stroke.

A CT scan was ordered and revealed that the man had experienced an ischemic stroke, meaning the blood supply had been cut off from the brain. The physicians at the hospital were unsure where the stroke originated at that time and scheduled a transesophageal echocardiogram, which is a procedure that captures pictures of the heart. The man was told to take two baby aspirins and return for the transesophageal echocardiogram less than one month later.

On Nov. 18, 2010, the man returned for the transesophageal echocardiogram. The procedure revealed the man's left ventricular function had been reduced by about 30–35%, which the physician believed indicated the man recently suffered a heart attack. He went back to the hospital two weeks later, which was the date of his previously and regularly scheduled visit with his primary care physician. The physician informed the man that the transesophageal echocardiogram revealed problems with

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 David Vassalli, co-authors, have no relevant relationships to disclose.

his heart and ordered a follow-up consultation with a cardiologist.

The physician noted in the records that the man most likely had a heart attack and prescribed him aspirin, atenolol, rosuvastatin, and a B12 vitamin. The next day, Dec. 2, 2010, the man suffered a catastrophic stoke that immediately led to the man suffering from locked-in syndrome.

The locked-in syndrome left the man a quadriplegic who has no voluntary muscle movement except for the ability to move his eyes and head on a limited basis. The man is also fully conscious but cannot speak, has to breathe through a tracheostomy tube, lost control of his bowels, and requires around-the-clock medical care. Later tests revealed that both strokes originated from the same place in the heart region.

The man filed a medical malpractice claim for negligent treatment by the staff at the veterans hospital between Oct. 21, 2010, and Dec. 2, 2010, which is the timeframe of when the symptoms were first presented and the second stroke occurred. Because this facility was a veterans hospital with federal funding, the United States was liable for the conduct of the hospital and its staff. The man alleged that the hospital was negligent because it failed to administer proper secondary stroke prevention. The man further alleged that he was not given the proper medications to reduce the likelihood of a second stroke.

The defense maintained that the man was given the proper care and medication. The defense further pointed out that this particular patient was uncooperative and stubborn in the past and an alternative medication regimen would not have been an option because it would require regular monitoring.

The judge rejected the defense's arguments and found the hospital failed to follow the necessary guidelines to prevent a second stroke. The judge awarded the man $21.5 million. The breakdown of the award was $13.3 million for medical care and expenses, $8.1 million in noneconomic damages, and $100,000 to the plaintiff's wife for her loss of consortium.

What this means to you: This case illustrates the need to follow guidelines set in place to prevent medical catastrophes. In this particular case that deals with a stroke patient, the court ruled that "[i]t is a basic principle of medicine that a patient who has suffered a stroke is generally at an elevated risk of suffering a second stroke. Therefore, doctors who are treating stroke patients must be cognizant of this risk, and they must take steps to prevent a second stroke."

The court went on to explain that "the established standard of care requires that a stroke patient undergo a thorough diagnostic evaluation to determine the cause of his stroke, and it requires that the patient be prescribed certain medication to treat the underlying condition that caused the stroke to occur." As the court's ruling explains, even while bearing in mind that the hospital staff considered this man stubborn and uncooperative, deviations from established standards can lead to massive liability.

This case also shows the danger of a physician making a judgment call regarding whether a patient will follow a recommended course of action.

The patient was not prescribed warfarin because the physician did not think he would take it due to the patient's past behavior. The court then did a balancing test and considered his past behavior, as well as evidence that suggested the man was "very likely taking Aspirin as prescribed [to him]" and family members testifying that the first stroke changed his health choices for the better. The court then determined it was "more likely than not" that he would have taken warfarin had it been prescribed to him.

The court balancing considerations demonstrates that a subjective judgment call, such as whether a patient will take his medication, later can be reconsidered by a court or jury and lead to liability. A physician seeking to limit liability in this circumstance would have explained to the patient the established standards regarding the proper medication to take, the risks involved with its proper and improper use, and the risks of not taking it at all, and the physician would have documented all of those communications. Then, unless the physician is certain that judgment call to deviate from the established standard will survive scrutiny, the physician should follow the established standard and prescribe the proper medication.

In this case, the physician made an assumption about the future compliance of this patient. Assumptions are a dangerous practice for physicians to make, yet they are, unfortunately, far from uncommon. The physician had an opportunity to inform the patient and close family members who would have been available to monitor compliance with anticoagulant use. This lost opportunity contributed to this unfortunate event and subsequent liability.

REFERENCE

United States District Court, D. New Hampshire. Case Number 13-cv-261-LM (April 03, 2015). ■

Hospital is held liable for nearly $2.8 million for misplaced tracheostomy

News: A 49-year-old woman was brought to the hospital after a car crash. She was unconscious and had internal bleeding with a lacerated liver. The hospital staff performed an endotracheal intubation and then successfully operated on the woman's liver. The woman remained at the hospital with the breathing tube in for a few days after the surgery. An ear, nose, and throat doctor (ENT), who was also an employee of the hospital, noticed swelling in her airway and recommended that the woman be given steroids and have a pulmonary consultation for extubation. According to the plaintiff's complaint, the surgeon administered a smaller amount of steroids than the ENT recommended, did not consult about an extubation, and instead performed a temporary tracheostomy.

The woman was released with the breathing tube, but she returned a few weeks later with an infection in the neck area where the tube was located. After consultation, the woman was sent to trauma surgeons at another hospital who unsuccessfully tried to repair damage that had occurred to the woman's vocal cords and larynx. As a result of the woman's damages, she requires a permanent breathing tube. The woman sued the hospital for the conduct of its staff. She specifically alleged that the surgeon was negligent for failing to conduct a pulmonary consultation before performing the tracheostomy and for failing to properly place the breathing tube lower. She also claimed that she was not given the amount of steroids that the ENT recommended. The defense argued that the woman's obesity made finding the proper placement very difficult and contributed to her being given a smaller amount of steroids than the ENT recommended. The jury agreed with the woman and found the hospital fully liable for the $2.8 million verdict.

> ... THE SURGEON ADMINISTERED A SMALLER AMOUNT OF STEROIDS THAN THE ENT RECOMMENDED, DID NOT CONSULT ABOUT AN EXTUBATION, AND INSTEAD PERFORMED A TEMPORARY TRACHEOSTOMY.

Background: In March 2009, a 49-year-old unconscious woman was involved in a car accident and brought to the hospital. She was bleeding internally and had a lacerated liver. To assist the woman's breathing during anesthesia, hospital staff performed an endotracheal intubation, which involves placing a breathing tube through the patient's mouth. The surgeon then successfully treated the woman's liver and internal bleeding. The breathing tube needed to remain in for a few days after the surgery. An ENT physician who worked at the hospital noticed swelling in the woman's airway and recommended that the woman be given 8 mg of steroids and have a pulmonary consultation for extubation, the removal of the breathing tube. Instead of the 8 mg of the steroids, the woman was given 4 mg, and according to the woman's complaint, the surgeon did not have a pulmonary consultation regarding extubation. Rather, the surgeon decided that the woman's neck was too thick and short and that the possible loss of airway made the procedure too risky. The surgeon then performed a temporary tracheostomy, which is an incision made in the windpipe through which a tube is inserted that assists the patient's breathing.

The woman was released and provided homecare instructions to change her breathing tube daily. A few weeks later, the woman returned to the hospital with an infection in the neck area where the tube was located. Physicians found tissue swelling, as well as an airway collapse and obstruction. They also determined that the breathing tube was placed too high.

The woman went to another hospital, where trauma surgeons found that the woman had suffered damage to her vocal cords and larynx. Surgeries to repair the damage were unsuccessful, which left the woman permanently requiring a breathing tube device to speak.

The woman filed a medical malpractice suit against the first hospital for the negligent acts of its staff. The woman alleged that the surgeon's conduct fell below the appropriate standard of care when the surgeon failed to request a pulmonary consultation before the tracheostomy and failed to place the breathing tube

in the proper place.

She also said that she was not given the dosage of steroids the ENT recommended. The defense argued that the fact that the woman was morbidly obese made proper placement very difficult and contributed to her being given a smaller amount of steroids than the ENT recommended. The defense further argued that the woman's need for a permanent breathing tube was caused by her not changing her breathing tube daily or following other homecare instructions. In a five-day trial, the jury found the hospital fully liable and awarded the woman $2.8 million, which broke down as just more than $1.6 million for pain and suffering and loss of wages, and just less than $1.2 million for future medical expenses.

What this means to you: There is a clear lesson from this case. Despite natural obstacles, such as a particularly short and thick neck making a procedure difficult, the standard of care that a physician is expected to provide still can be breached when the physician doesn't comply with recognized standards. Neglecting to consult with a pulmonologist before performing the tracheostomy, as recommended, was the first breach of the standard of care.

While it might have been obvious to the surgeon that weaning the patient off intubation probably would not be possible, the documented support of a pulmonologist likely would have lessened the surgeon's liability. More generally, physicians too frequently neglect to seek the consultations of their peers to support difficult decisions made in complicated cases. In this case, the patient's obesity and thick, short neck made placing the tracheostomy incision at the desired location, through the second, third, and fourth tracheal ring, difficult. This difficulty resulted in the woman's damages from the tracheostomy incision being through the first tracheal ring and the cricoid cartilage. While the surgeon noted that the woman's neck made placement difficult, the surgeon's report incorrectly stated that the incision was made through the second, third, and fourth tracheal ring. Here again, the surgeon might have asked for the assistance of another surgeon with experience performing difficult tracheostomies.

This effort would have shown the surgeon's concern for the patient and his efforts to provide her with an optimal outcome.

Another way the surgeon and hospital could have better sheltered themselves from liability would have been to also report every step taken to properly place the tracheostomy, as well as any postoperative concerns.

A report reading that the surgeon took every step to best place the tracheostomy and provided a detailed explanation of where the incision was made and possible outcomes that might occur would have shown due diligence on the part of surgeon and hospital. This information would have provided evidence to the jury that the hospital and its staff made their best efforts to overcome a natural obstacle, and it likely would have resulted in less liability, or perhaps no liability, for the hospital.

There is another example demonstrating that physicians and hospitals seeking to shelter themselves from liability should keep detailed and accurate records. That example is the issue of the ENT's recommendation. The woman's complaint points out that the pulmonary consultation recommended by the ENT as an alternative to the tracheostomy never occurred, and the surgeon moved forward with the tracheostomy without following a colleague's recommendation.

The surgeon maintained that the recommendation was "discussed" and determined to be too risky due to the woman's medical condition.

However, there was no recording in the patient's file about the surgeon following through with the ENT's recommendation, and there was no detailed and thorough explanation as to why the specific course of action was chosen. Thus, the woman's attorney could use the patient's file to create the narrative that the surgeon disregarded a fellow physician's recommendation and carelessly moved forward with an unnecessary surgery that was compounded by additional carelessness.

A complete and legally useful record for the surgeon and hospital could have rebutted that narrative if the record had included certain items. Those items include the interdepartmental recommendations and the primary team's considerations, a description of intent regarding the chosen course of action and possible outcomes, and supplemental reports that include new developments or considerations and demonstrate attentiveness to the patient's condition. Furthermore, keeping a detailed record and filing of supplemental reports as a means of avoiding liability become an even more effective tool when dealing with patients who present unique and difficult obstacles, as medical errors and the legal liability are more likely to occur in these scenarios.

REFERENCE

Court of Common Pleas of Delaware County, Pennsylvania. Case Number 2011-002362 (Aug. 24, 2015). ■