HEALTHCARE RISK MANAGEMENT™

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

INSIDE

AHC Media

AUGUST 2015 Vol. 37, No. 8; p. 85-96

When does a hospital's apology switch to being manipulation?

Concerns raised that hospitals use 'I'm sorry' to evade responsibility

Risk managers have largely embraced the idea of apologizing after an adverse event and communicating fully with the patient or family members, in no small part because this approach has been proven to reduce malpractice costs. In addition, it just seems the right thing to do and promotes a positive image of the hospital.

But can this well-intentioned theory go wrong? Can potential plaintiffs be unfairly manipulated by savvy hospital leaders and attorneys who know how to influence them to the hospital's advantage?

It happens, says **Steve S. Kraman**, MD, a professor of internal medicine at the University of Kentucky College of Medicine in Lexington. He is an outspoken critic of what he says has too often become a crass maneuver to save the hospital money by denying people the compensation that they rightly deserve after an adverse event.

> "THERE ARE FACILITIES OUT THERE THAT ARE USING THIS AS A STRATEGY TO SAVE MONEY: 'SAY YOU'RE SORRY, PAY SOME MONEY, AND THEY'LL GO AWAY.'"

Kraman instituted one of the first formal apology programs, sometimes known as "communication and resolution," in 1987 when he was chief of staff at the Veterans Affairs hospital in Lexington. That program helped spur the nationwide "Sorry Works" campaign that encouraged all hospitals to adopt the same approach of acknowledging the adverse event quickly, communicating fully with the

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 1.25 nursing contact hours using a 60-minute contact hour.

Provider approved by the California Board of Registered Nursing, Provider #CEP14749, for 1.25 Contact Hours.

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

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

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

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

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

patient or family, and apologizing when appropriate. *(For more on the "Sorry Works" approach, see* Healthcare Risk Management, *October 2011, pp. 109-113.)*

The program significantly lowered the malpractice costs of the VA hospital. From 1990 to 1996, Kraman's VA hospital had 88 claims and paid an average $15,622 per claim, compared with a $98,000 average at VA hospitals without "I'm sorry" policies. That result got the attention of hospital leaders and helped spread the program to many other health systems. However, those cost savings were never the real intent of the program, Kraman says, and that's where hospital leaders can go wrong.

Theory watered down

Kraman's approach over 16 years at the VA hospital was to investigate the adverse event before talking to the patient or family, and then tell them everything. The emphasis was on full disclosure of whatever happened and how the hospital or clinicians might have erred.

"But at the same time, and we did this from the very beginning, we advised them always to hire an attorney," Kraman says. "Even though we had every intention of doing well by them, there was clearly such an imbalance of power that we didn't think it was fair for them not to have an attorney."

Kraman's practice was to suggest an attorney at the point when it was necessary to discuss compensation, not in the first conversations to explain what happened. Over the years, the original approach has been watered down to a more simplistic idea that if you talk to the potential plaintiffs and appear contrite, they won't sue you, he says. That approach can lead to the false idea that suggesting an attorney runs counter to what you're trying to achieve.

Saving money is not the point, Kraman says. Rather, the goal is to resolve the problem fairly and as quickly as possible, while avoiding litigation. Saving money almost certainly will be a side benefit, but it is not the primary goal. That wording might be a fine distinction, but it matters in how the policy is executed, he says.

"There are facilities out there that are using this as a strategy to save money: 'Say you're sorry, pay some money, and they'll go away,'" Kraman says. "Patients become very malleable when you treat them this way, and someone who doesn't have a lot of professional morals can take

EXECUTIVE SUMMARY

The "communication-and-resolution" approach after an adverse event has been shown to reduce malpractice costs, but some critics say it can unfairly manipulate the patient and family. Lower malpractice costs should be only one goal of the approach.

- Some say the patient always should be encouraged to retain an attorney before any significant discussions.
- Adhering to the original method of apologizing might eliminate the risk of unfair manipulation.
- It might be acceptable for hospitals to settle directly with patients rather than through a lawyer.

advantage of people. They're taking unfair advantage of the way people's lack of knowledge and goodwill can lead them to bad decisions."

In his experience at the VA, Kraman saw cases in which the patient was so impressed by the apology that they wouldn't take compensation that they were rightly due for their injuries. Hospital attorneys had to explain to them that they were not hurting anyone's feelings and persuade them to accept compensation, Kraman says.

Lawyer not needed?

Poor execution of the approach can indeed lead to taking advantage of vulnerable people, says **Richard C. Boothman**, JD, chief risk officer and executive director of clinical safety at the University of Michigan Health System (UMHS) in Ann Arbor, which Kraman cites as an example of a health system that handles communication and resolution properly. The University of Michigan Health System has encouraged doctors since 2002 to apologize for mistakes. In the next two years the system's annual attorney fees have dropped from $3 million to $1 million, and malpractice lawsuits and notices of intent to sue fell from 262 filed to about 130 per year, Boothman reports. *(More information on the UMHS model and results is available online at http://tinyurl.com/pdycc8n.)*

Taking advantage of people would be "completely counterproductive to our goals," Boothman says. UMHS has even compensated people who could not sue because the statute of limitations had run out, he says.

"It is so important for us to demonstrate to our staff that accountability for medical injuries due to errors is a priority," Boothman says. "Cheating someone just because we could is completely anathema to what we are trying to do. The goal for us from day one has not been to save money on malpractice but to establish accountability for preventable medical errors."

Boothman, a former trial attorney himself, agrees that patients and family should be encouraged to obtain a lawyer, and UMHS insists on representation if a minor is involved or the case involves substantial compensation. Boothman keeps a list of law firms with which UMHS has worked constructively and recommends them to any patient or family seeking counsel, but he says there are situations in which it is reasonable for the patient or family to forgo an attorney.

"Those who say we must always have a lawyer present are disrespectful of patients who are smart enough to say they don't want to give up a third of their settlement to a lawyer," Boothman says. "It's also a cynical view of the world to say we have to read Miranda rights to everybody before we can maintain the patient/physician relationship and come to a resolution with someone who's been hurt."

Let lawyers do paperwork

Kraman is less willing to accept a patient or family's refusal to get a lawyer. Though he has settled with patients who declined to obtain an attorney, Kraman says those situations always made him uneasy.

"Patients are not on an equal playing field," he says. "The hospitals, the doctors, the insurers all have more knowledge and resources. They also have the ability to predict future needs the patient may not be aware of, or to withhold that information. The hospitals and attorneys may be completely trustworthy and trying to do the right thing, but they have split allegiances, and the patient is not their client."

In that situation, a patient might walk away feeling like he or she received a good settlement, but the patient might realize years later that it is not adequate to cover disabilities and medical costs, Kraman says. In addition, he notes that hospital attorneys usually find it more productive to negotiate terms with another attorney.

Encouraging a patient or family member to seek a lawyer should be handled carefully, says **Rodney K. Adams**, JD, an attorney with the law firm of LeClair Ryan in Richmond, VA. There is a risk of polarizing the situation more than necessary if you convey that the hospital's actions were so egregious that lawyers are needed to sort it out and protect the patient's rights, he says. A more deft approach would be to explain that legal representation is advised even when the two parties are amicable and willing to reach a fair resolution, he says. The message should be that even in a good settlement, lawyers are necessary to handle the legal details and paperwork, he says.

"In those situations, adding a lawyer to the mix doesn't have to create a more contentious environment or result in more liability for the hospital," he says. "It will, however, have everyone walking away more satisfied that everyone's rights were protected."

SOURCES

- Richard C. Boothman, JD, Chief Risk Officer, University of Michigan Health System, Ann Arbor. Email: boothman@med.umich.edu.
- Steve S. Kraman, MD, Professor of Internal Medicine, University of Kentucky College of Medicine, Lexington, KY. Email: sskram01@email.uky.edu. ■

Warning! Audio/video recordings could be a liability risk for your hospital

Smartphones are everywhere, and it has become increasingly common for patients to record their encounters with clinicians, usually so they can review the medication instructions or other information that they might not remember clearly. Patients also find it useful to show spouses or caregivers the recording so they have a clear understanding of what transpired.

Those recordings could be a liability risk. Much like the 1990s controversy over whether to allow videotapes of childbirth, some legal experts caution that the recording could be used against the clinicians in a malpractice case. But not everyone agrees that the risk outweighs the positive aspects.

A jury recently awarded a patient $500,000 after he accidentally recorded clinicians making disparaging remarks about him during surgery. He had hit "record" on his smartphone before surgery so he could review the post-op instructions, but he forgot to turn off the phone. It was with his personal belongings underneath the surgery table. *(See the story in this issue for more details and a link to the audio of the recording.)*

Most hospitals have prohibited recording in childbirth, but the video recordings still are entered into evidence occasionally in malpractice cases, notes **David M. Walsh IV**, JD, partner with the law firm of Chamblee Ryan in Dallas. "The family sneaks the camera in inside a bag or a teddy bear and records the birth," he says. "The videos end up being a mixed bag, with the plaintiff's experts seeing what they want to see in it, and the defense experts seeing what they want to see. Nonetheless, the defense usually isn't happy to see one introduced as evidence, because you never know how a lay jury is going to react to what they see on screen."

> "UNLESS IT IS SOMETHING VERY SPECIFIC AND LIMITED, LIKE A DOCTOR TELLING YOU HOW TO TAKE A CERTAIN MEDICATION, I WOULD SUGGEST NOT ALLOWING THEM TO BE RECORDING YOU."

One of the primary concerns with childbirth videos is that jurors might overreact to what they see in the video because childbirth can be messy, with plenty of blood, fluids, and clinicians talking in jargon they might not understand. It would be easy for jurors to conclude something was wrong even if experts testify otherwise.

With more sedate patient encounters in the office, that might not be a problem. Still, video recordings can be misleading if they do not capture the entire interaction perfectly, which no smartphone can, Walsh says. The recording might have audio of the doctor giving instructions to the patient, for example, but it might not capture the patient nodding to indicate comprehension, or it might not show what written material was provided.

Lawyer: Don't do it

Walsh advises not allowing patients to record encounters with clinicians.

"Unless it is something very specific and limited, like a doctor telling you how to take a certain medication, I would suggest not allowing them to be recording you," Walsh says. "If they want to record you generally, the entire encounter, that tells me they don't trust you for some reason, and that would make me suspicious of their motivation."

Some clinicians see more benefit than risk in allowing patients to record their encounters. **Randall W. Porter,** MD, a surgeon with Barrow Neurological Associates in Phoenix,

EXECUTIVE SUMMARY

More patients are using smartphones to record their interactions with clinicians. Allowing such recordings could place the hospital and clinicians at risk of a malpractice lawsuit.

- A recent verdict involved a patient who recorded clinicians making disparaging remarks during surgery.
- Some physicians encourage the recordings to improve patient understanding and compliance.
- Recordings are unlikely to be a complete record of the encounter.

AZ, encourages his patients to record their interactions. He was prompted in part by his father's experience with prostate cancer. Although his father had a PhD in economics and his mother was a nurse, Porter could tell that they recalled only part of what was said when talking with a clinician.

"A lot of factors go into that: information overload, emotionally charged discussions, age, hearing loss, medications," Porter says. "I figured if I would have liked to have a recording for my own father, why not offer it to my own patients?"

Porter eventually went a step further and started recording patient encounters himself and offering the patient a copy. He has developed a recording system called the Medical Memory, which uses a computer tablet. Patients create an account on the tablet, which is then placed on a stand in the examination room. The doctor starts and stops the recording, after which a copy is automatically sent to the patient. The cost of the system varies according to a practice's needs, but an office utilizing two systems for clinic, rounding, and discharge is charged about $300 a month, which includes the hardware. *(More information is available online at http://www.themedicalmemory.com.)*

"We've done over 4,000 patients with about 20 providers using it, and we've never had a legal issue, no 'gotcha' moment," Porter says.

SOURCES

- Randall W. Porter, MD, Surgeon, Barrow Neurological Associates, Phoenix, AZ. Email: Randall.Porter@bnaneuro.net.
- David M. Walsh IV, JD, Partner, Chamblee Ryan, Dallas. Telephone: (214) 905-2003. ■

Anesthesiologist ordered to pay $500,000 after patient's smartphone records insults

After a three-day trial, a Fairfax County, VA, jury ordered an anesthesiologist and her practice to pay a patient $500,000 for disparaging remarks made during surgery and a false diagnosis on his chart. The man might never have known about the offenses if he had not accidentally recorded the encounter on his smartphone.

The comments were made by anesthesiologist Tiffany M. Ingham, MD, an employee of the Aisthesis anesthesia practice in Bethesda, MD, which the jury ruled should pay $50,000 of the $200,000 in punitive damages it awarded. Court records identify the plaintiff only as D.B., but they tell a story that illustrates how smartphone recordings can expose healthcare providers to significant liability.

D.B. was preparing for a colonoscopy in a Reston, VA, surgical center when he started a recording on his smartphone so he could capture the physician's instructions to him. His phone was put in his personal belongings in a bag underneath the surgical table, still recording throughout the entire procedure, court records indicate.

When he reviewed the recording, he was shocked to hear the surgical team insulting him, mocking him, and falsifying a diagnosis. These are some of the comments on the recording:

• "After five minutes of talking to you in pre-op I wanted to punch you in the face and man you up a little bit," the anesthesiologist said.

• A medical assistant noted the man had a rash, and the anesthesiologist warned her not to touch it. She cautioned the assistant that she might get "some syphilis on your arm or something."

She added, "It's probably tuberculosis in the penis, so you'll be all right." Others in the room laughed at the remark. The gastroenterologist said, "As long as it's not Ebola, you'll be fine." The anesthesiologist joked "It's penis Ebola," which prompted more laughter.

• The assistant recounted how the man said he always passed out when watching a needle placed in his arm. The anesthesiologist said, "Well, why are you looking then, retard?"

• The gastroenterologist told the medical assistant that she should speak to the patient after surgery and lie to the patient about the doctor having been there.

"Just tell him Dr. Shah said everything, and you just don't remember it," he said. The anesthesiologist then suggested that the doctor have a "fake page" go off as an excuse not to talk to the patient. She said she has used fake pages before.

• Again debating who would have to talk to the patient after the procedure, the anesthesiologist said, "Round and round we go, wheel of annoying patients we go. Where it lands nobody knows."

• The anesthesiologist said, "I'm going to mark hemorrhoids even though we don't see them and probably won't. I'm just going to take a shot in the dark." (*The audio recording is available online at http://tinyurl.com/og37fez.)* ■

Revamped RRT and early warning system improves safety at pediatric hospital

An early intervention is often the best strategy for keeping patients healthy, and a pediatric hospital is reporting improved patient safety from an early warning system that helps identify patients most at risk for a gradual but severe decline toward being critically ill.

The Ronald McDonald Children's Hospital (RMCH) at Loyola University Medical Center in Maywood, IL, also has revamped its rapid response team (RRT) as part of an overall effort to improve patient safety, says **Julie Fitzgerald**, MD, FAAP, division director of Loyola University Health System's pediatric intensive care medicine unit and associate professor in the Department of Pediatrics at Loyola University Chicago Stritch School of Medicine.

"Children can become critically ill from sudden and unexpected events, but more often it is a gradual progression arising from various illnesses, which leaves a large window of opportunity to identify children at-risk in our children's hospital," Fitzgerald explains.

RMCH used the Cardiac Children's Hospital Early Warning Scoring (C-CHEWS) tool developed at Boston Children's Hospital. It focuses on three areas: neuro/behavioral, respiratory, and cardiovascular. Patient-specific concerns from the family and nursing staff also are taken into account for each child's score. The child is evaluated using a specific nursing and physician response algorithm, and each patient is given a score from 0-10. A score is given every four hours, along with each set of vitals. *(C-CHEWS is described fully in a report in the* Journal of Pediatric Nursing. *An abstract and access to the full text is available online at http://tinyurl.com/otzsc7b.)*

RMCH introduced the C-CHEWS system in April 2015, so Fitzgerald says it's too early to assess the results. But she also introduced the system at another pediatric hospital before coming to RMCH, and she says the effects there were significant. Fitzgerald saw the same benefits that Boston Children's Hospital has reported in the literature: a reduction of mortality rates, improved clinical outcomes and decreased length of stay, better awareness of physiological deterioration or instability, and improved safety and satisfaction for patients, their families, and the children's hospital staff.

The C-CHEWS system was developed in part to address in-house cardiac arrest and serious clinical decompensation that necessitates transferring children to an intensive care setting, she explains. Those problems can develop suddenly but more often are the result of a slow decompensation over hours or even days. "That gives us this large window of opportunity to identify those changes and perhaps intervene earlier so that the child doesn't have that catastrophic event," Fitzgerald says. "But with shift changes and patient handoffs, you can miss some of that slow slide downward over time. These early warning systems provide an objective score that can alert the staff to the patient who is on that path even if they haven't put the clues together yet."

Other scoring systems also are available and seek the same result, but Fitzgerald says RMCH and her previous hospital selected C-CHEWS because it not only scores the objective findings of clinical changes, but it also includes subjective findings from observers. "You can get a bonus point if the parents are worried, and you can get a bonus point if the nurse is worried," she explains. "It incorporates those subjective, gut feelings that sometimes are important in medicine, when the nurse says, 'I can't put my finger on it, but something has changed with this child. Something is not right.'"

Protocol changed

Implementing this system also spurred a revamping of the hospital's rapid response team (RRT). Previously, the RRT was not called

EXECUTIVE SUMMARY

A pediatric hospital has improved patient safety by implementing an early warning system that encourages earlier intervention with high-risk patients. The hospital also improved its rapid response team (RRT).

- Patients are scored every four hours on clinical measures, plus the subjective feelings of nurses and family members.
- The scores are color-coded to dictate the appropriate response, with the worst scores prompting an immediate RRT call.
- The system encourages residents to see patients in person more often, rather than relying mostly on data at a computer station.

out until a patient was confirmed to be in serious distress, Fitzgerald says. As a result, almost all RRT calls ended with the patient being transferred to the pediatric intensive care unit (PICU).

"That's not the best way for a rapid response team to work," Fitzgerald says. "If we can respond sooner and intervene in time, we can keep these kids from deteriorating to the point that the PICU is the only right choice."

RMCH uses a color-coding system for the scores to indicate what action should be taken. A score of 0-2 is green, meaning the patient is stable and the staff can continue routine care and scoring every four hours. A score of 3-4 is yellow, prompting the staff to notify residents that the patient needs to be evaluated. Residents are expected to evaluate the child within 10 minutes of that notification, including a discussion with the parents. A yellow score also means the patient will be scored every two hours, instead of every four, for two rounds to make sure this score is not the beginning of a more rapid deterioration.

A total score of 5 or greater, or a score or 3 or greater in any single domain, triggers a mandatory activation of the RRT, which includes the senior resident in the PICU, the charge nurses, and a respiratory therapist. The RRT team must be at the bedside within five minutes to assess the patient, talk to the family, and intervene as necessary. The resident must contact the PICU attending directly to agree on whether the patient can stay on the unit or be moved immediately to the PICU.

If the patient stays on the floor, scoring is performed hourly, and the resident re-evaluates the child again until the score drops. Each hourly scoring and assessment includes a decision to keep the child on the floor or move to the PICU.

"This gets residents up and away from the computer. It's easy to sit there and look at the numbers and labs all night long without actually going out there to be on the floors and see the patients and see the nurses," Fitzgerald says. "It gets the kids on people's radar, especially those who might be a little more fragile and who may need a closer look to understand what's really going on."

SOURCE

- Julie Fitzgerald, MD, FAAP, Division Director of Pediatric Intensive Care Medicine, The Ronald McDonald Children's Hospital at Loyola University Medical Center, Maywood, IL. Email: julie.fitzgerald@lumc.edu. ■

RCAs become RCA2s under new NPSF guidelines

Analysis is good, but acting on that information is what really makes a difference. That's the message from the National Patient Safety Foundation (NPSF) in Boston, which has revised its guidelines for conducting a root cause analysis (RCA).

The guidelines, *RCA2: Improving Root Cause Analyses and Actions to Prevent Harm*, have been endorsed by several related organizations and is being widely distributed to hospitals, health systems, and other settings. The American Society for Healthcare Risk Management did not endorse the guidelines or participate in their development. (*The guidelines are available online at http://tinyurl.com/prhkxv9.)*

With a grant from The Doctors Company Foundation, the NPSF convened a panel of subject matter experts and stakeholders to examine best practices around RCAs and develop guidelines to help health professionals standardize the process.

"We've renamed the process RCA2 — RCA squared — with the second "A" meaning action, because unless real actions are taken to improve things, the RCA effort is essentially a waste of everyone's time," co-chair of the panel **James P. Bagian**, MD, PE, explained when the guidelines were announced. Bagian is a member of the NPSF Board of Governors and director of the Center for Health Engineering and Patient Safety at the University of Michigan in Ann Arbor. "A big goal of this project is to help RCA teams learn to identify and implement sustainable, systems-based actions to improve the safety of care," Bagian said.

One member of the panel was **Ailish M. Wilkie**, MS, CPHRM,

EXECUTIVE SUMMARY

The National Patient Safety Foundation (NPSF) has revised its guidelines for conducting root cause analyses.

- The "A" in the acronym has been emphasized to indicate the need for action in addition to analysis.
- The analysis should include reporting back to whoever initially reported the event.
- Those directly involved in the event should be excluded from the analysis.

CPHQ, senior project manager in patient safety and risk management with Atrius Health Patient Safety & Risk Management, a non-profit alliance of health systems in Massachusetts. She and the other panel members concluded that risk managers and other healthcare leaders often fall short in acting on what they found during an RCA.

"We do a great job of performing RCAs, but the actions and the measurement of those improvement actions is something that we all have an opportunity to improve," Wilkie says. "Standardizing how we do RCAs, by following the NPSF process, will help us all conduct more successful RCAs."

The action part of an RCA should include closing the loop with staff or physicians who reported the event, she says. Risk managers must counter the common notion that any concerns reported to administration disappear in a black hole and are never heard again, Wilkie says. Communicating with those individuals about the RCA's findings will encourage people to report their concerns more often in the future, she says.

Elevating the RCA process might be most challenging for smaller hospitals, she says, for the same reason that they already might find it difficult to do a thorough RCA: lack of staff, time, and other resources. The revised NPSF guidelines should be useful for smaller facilities, nonetheless, because they provide a framework that can make RCAs consistent from one facility to another, regardless of size, she says.

"The guidelines also can help us get back to some of the best methodology that we might have done when we first started conducting RCAs but which have fallen out of practice along the way," Wilkie explains. "For instance, the new guidelines suggest that the individuals who are directly involved in the event not be part of the RCA team. That might have been a best practice in the beginning, but some smaller organizations can find it hard to exclude the people directly involved because that person might be the only one in the department."

"STANDARDIZING HOW WE DO RCAs, BY FOLLOWING THE NPSF PROCESS, WILL HELP US ALL CONDUCT MORE SUCCESSFUL RCAs."

Those directly involved in the event should be excluded from the RCA whenever possible because they might come to the table with preconceived ideas, Wilkie explains. Ideally, every RCA participant should begin with no preconceptions about what happened or why, which is a goal that is more easily met by a large organization with many people qualified to participate, she says.

The NPSF guidelines also emphasize that some adverse events are not appropriate for an RCA.

"RCA2 processes are not to be used to focus on or address individual health care worker performance as the primary cause of an adverse event, but instead to look for the underlying systems-level causations that were manifest in personnel-related performance issues," the guidelines state. "A common definition of blameworthy events includes events that are the result of criminal acts, patient abuse, alcohol or substance abuse on the part of the provider, or acts defined by the organization as being intentionally or deliberately unsafe."

Start within 72 hours

The new guidelines encourage beginning an RCA within 72 hours, but Wilkie notes that the NPSF doesn't necessarily mean convening the investigators for the first meeting of the RCA team within that time. Rather, the initial investigation should begin within that time limit by reviewing the patient chart and creating a timeline of events.

"That's something that can be done by the risk manager and doesn't need the RCA team as a whole," Wilkie says.

Another new emphasis is on the idea that an RCA is a normal part of work for those involved, rather than seeing it as something abnormal and outside the regular scope of work. For example, NPSF recommends that RCA sessions be held during normal business hours and treated as an ordinary part of the employee's time at work. That approach helps prevent staff from seeing the RCA process as a burden or added duty, Wilkie says.

"Sometime physicians can't meet with you during normal hours because they're too busy with patients, so convening after hours might be unavoidable," Wilkie says. "But to the extent you can, you want to foster the idea that and RCA is an important but standard part of what we do to improve quality and safety."

SOURCE

- Ailish M. Wilkie, MS, CPHRM, CPHQ, Atrius Health Patient Safety & Risk Management. Newton, MA. Telephone: (617) 559-8269. Email: ailish_wilkie@atriushealth.org. ■

Never events usually are traced to multiple human factors, not just a root cause

Researchers at the Mayo Clinic in Rochester, MN, have confirmed what many risk managers have noted from their own root cause analyses: Most never events can be traced back to human factors rather than just a root cause.

Most commonly, the researchers found, never events are caused by between four and nine human factors.

They identified 69 never events among 1.5 million invasive procedures performed over five years, and they detailed why each occurred. Using a system created to investigate military plane crashes, they coded the human behaviors involved to identify any environmental, organizational, job, and individual characteristics that led to the never events. They found that 628 human factors contributed to the errors overall, roughly four to nine per event. The study results are published in the journal *Surgery*. *(An abstract and access to the full text of the study are available online at http://tinyurl.com/pj5nweb.)*

The never events included performing the wrong procedure (24), performing surgery on the wrong site or wrong side of the body (22), leaving an object in the patient (18), or putting in the wrong implant (5). All of the errors analyzed occurred at Mayo, and none were fatal.

The Mayo Rochester campus rate of never events over the period studied was roughly one in every 22,000 procedures, notes senior author **Juliane Bingener**, MD, a gastroenterologic surgeon at Mayo Clinic. Because of inconsistencies in definitions and reporting requirements, she says, it is hard to find accurate comparison data, but a recent study based upon information in the National Practitioner Data Bank estimated that the rate of such never events in the United States is almost twice that in this report, approximately one in 12,000 procedures.

Nearly two-thirds of the Mayo never events occurred during relatively minor procedures such as anesthetic blocks, line placements, interventional radiology procedures, endoscopy, and other skin and soft tissue procedures.

Despite increasing attention from the medical community, eradicating never events entirely remains elusive, Bingener says. The findings indicate that the never events were not often tied to "cowboy-type" behavior from physicians or staff who disdained safety efforts or casually violated protocols, she notes.

"What it tells you is that multiple things have to happen for an error to happen," Bingener says. "We need to make sure that the team is vigilant and knows that it is not only OK, but is critical that team members alert each other to potential problems. Speaking up and taking advantage of all the team's capacity to prevent errors is very important, and adding systems approaches as well."

For example, to help prevent surgical sponges from being left in patients, Mayo Clinic installed a sponge-counting system with bar code-scanning to track sponges. The hospital also emphasizes use of The Joint Commission's Universal Protocol, team briefings and huddles before a surgery starts, a pause before the first incision is made, and debriefings using a World Health Organization-recommended safety checklist. *(The WHO checklist is available online at http://tinyurl.com/ocofcbv.)*

To investigate the never events, the researchers used human factors analysis, a system first developed to investigate military aviation accidents, Bingener explains. They grouped errors into four levels that included dozens of factors:

- **"Preconditions for action,"** such as poor hand-offs, distractions, overconfidence, stress, mental fatigue, and inadequate communication. This category also includes channeled attention on a single issue. In layman's terms, that wording means focusing so much on a tree that one cannot see the forest.
- **Unsafe actions,** such as bending or breaking rules or failing to understand. This category includes perceptual errors such as confirmation bias, in which surgeons or others convinced themselves they were seeing what they thought they should be seeing.
- **Oversight and supervisory factors** including inadequate supervision, staffing deficiencies, and planning problems, for example.
- **Organizational influences** such as problems with organizational culture or operational processes.

In addition to systems approaches and efforts to improve communication, attention should be paid to cognitive capacity, such as team composition, technology interfaces, time pressures, and individual fatigue, the researchers say.

SOURCE

- Juliane Bingener, MD, Gastroenterologic Surgeon, Mayo Clinic, Rochester, MN. Telephone: (480) 301-7033. ■

OSHA promises closer scrutiny of staff injuries

The Occupational Health and Safety Administration (OSHA) is cracking down on injuries to nurses and other healthcare staff members. In particular, OSHA inspectors will monitor and investigate hospital efforts to prevent injuries to nurses during patient lifting.

The agency has issued recommendations in the past for avoiding lifting injuries in healthcare settings, but the new statement from OSHA makes clear that healthcare providers can be fined for noncompliance. The stronger enforcement stance comes after an April 2015 report that found a sharp increase in healthcare workplace injuries.

The report is available online at http://tinyurl.com/oosp3j6. OSHA's recommendations for injury prevention are available at http://tinyurl.com/nak93gg.

In announcing the crackdown, the agency noted that hospitals have acknowledged the threat of injuries while lifting patients and encouraged "body mechanics" strategies, such as straight-backed, knees-bent lifting. However, OSHA said research indicates that these methods are not enough to prevent injuries. It says the only proven method thus far is using special equipment to lift patients.

OSHA has advised its staff members through a memorandum that all inspections of hospitals and nursing home facilities, including those prompted by complaints, referrals, or severe injury reports, should include the review of potential hazards related to the following categories:

- patient handling;
- bloodborne pathogens;
- workplace violence;
- tuberculosis;
- slips, trips, and falls.

You can see the memorandum at http://tinyurl.com/nokcbgn. ■

243 people arrested for $712 million in false billing

In a case involving the most defendants charged and largest alleged loss amount in the history of the federal fraud task force, a nationwide sweep has led to charges against 243 individuals, including 46 doctors, nurses, and other licensed medical professionals, for their alleged participation in Medicare fraud schemes involving approximately $712 million in false billings.

Department of Health and Human Services (HHS) Secretary Sylvia M. Burwell and Attorney General Loretta E. Lynch announced the charges. In addition, the Centers for Medicare & Medicaid Services also suspended several providers using its suspension authority as provided in the Affordable Care Act.

The defendants are charged with various healthcare fraud-related crimes, including conspiracy to commit healthcare fraud, violations of the anti-kickback statutes, money laundering, and aggravated identity theft. The charges are based on alleged fraud schemes involving medical treatments and services, including home health care, psychotherapy, physical and occupational therapy, durable medical equipment, and pharmacy fraud. More than 44 of the defendants arrested are charged with fraud related to the Medicare prescription drug benefit program known as Part D, which is the fastest-growing component of the Medicare program overall.

According to court documents, the defendants participated in alleged schemes to submit claims to Medicare and Medicaid for treatments that were medically unnecessary and often never provided. In many cases, patient recruiters, Medicare beneficiaries, and other co-conspirators allegedly were paid cash kickbacks in return for supplying beneficiary information to providers, so that the providers could submit fraudulent bills to Medicare for services that were medically unnecessary or never performed.

"Every day, the Criminal Division is more strategic in our approach to prosecuting Medicare fraud," said Assistant Attorney General **Leslie R. Caldwell**, JD, of the Justice Department's Criminal Division. "We obtain and analyze billing data in real time. We target hotspots — areas of the country and the types of healthcare services where the billing data shows the potential for a high volume of fraud — and we are

COMING IN FUTURE MONTHS

- Scribes: Good or bad for risk?
- Standardizing emergency codes
- Avoiding wrong-site errors
- Preventing fires in the operating room

speeding up our investigations. By doing this, we are increasingly able to stop schemes at the developmental stage and to prevent them from spreading to other parts of the country."

The Medicare Fraud Strike Force operations are part of the Health Care Fraud Prevention & Enforcement Action Team (HEAT), a joint initiative announced in May 2009 between the Department of Justice and HHS to focus their efforts to prevent and deter fraud and enforce current anti-fraud laws around the country. Strike Force operations in nine locations have charged more than 2,300 defendants who collectively have falsely billed the Medicare program for more than $7 billion. ■

Study: Aggressive med mal increases LOS and costs

Patients who undergo spine surgery in a community known to be an aggressive malpractice environment are likely to be hospitalized longer and incur higher charges, according to a study published recently in *The Spine Journal*.

Researchers from Louisiana State University in Shreveport and Dartmouth – Hitchcock Medical Center in Lebanon, NH, examined the correlation of malpractice liability with unfavorable outcomes in spine surgery. Data were included for 707,951 patients undergoing spine surgery who were registered in the Nationwide Inpatient Sample database from 2005 to 2010. Measures of volume and size of the malpractice claim payments were created using data pulled from the National Practitioner Data Bank.

The researchers found a correlation for higher number of claims per 100 physicians in a state with increased hospitalization charges and length of stay. No correlation was seen for mortality. There was a correlation between larger magnitude of awarded claims and increased hospitalization charges and length of stay, according to the researchers.

An abstract and access to the full text of the study are available online at http://tinyurl.com/ps48zew. ■

Hospitals sued over claims they limited marketing

The Department of Justice (DOJ) sued four hospital systems that it says for years unlawfully agreed to allocate territories for marketing, which it says denied consumers and physicians important information about competing providers and other benefits of unfettered competition.

Three of the systems — Hillsdale (MI) Community Health Center; Community Health Center of Branch County, MI, and ProMedica Health System in Toledo, OH — agreed to settle the charges. DOJ continues to litigate against W.A. Foote Memorial Hospital in Jackson, MI, now doing business as Allegiance Health, to prohibit agreements that unlawfully allocate territories for marketing of competing healthcare services.

Hillsdale, Allegiance, Community Health Center, and ProMedica's Bixby and Herrick hospitals — the only hospitals in their respective counties — each competed through marketing to attract patients. The complaint alleges that Hillsdale curtailed this competition for years by entering into agreements with Allegiance, Community Health Center, and ProMedica to limit the marketing of competing services. According to the complaint, the defendants' agreements deprived patients and physicians of information needed to make informed healthcare decisions. Patients in Hillsdale County, MI, also were prevented from receiving free medical services, such as health screenings and physician seminars, that they would have received from Allegiance in the absence of its unlawful agreement with Hillsdale.

The proposed settlement prohibits Hillsdale, Community Health Center, and ProMedica from agreeing with other health providers, including hospitals and physicians, to limit marketing or to divide any geographic market or territory. The proposed settlement also prohibits communications among the defendants about their marketing activities, subject to limited exceptions. These hospitals also will implement compliance measures to prevent anticompetitive practices. ■

CNE OBJECTIVES

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

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

HEALTHCARE RISK MANAGEMENT™

CNE INSTRUCTIONS

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

2. Scan the QR code to the right or log on to the 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 QUESTIONS

1. According to Steve S. Kraman, MD, a professor of internal medicine at the University of Kentucky College of Medicine, when is the right time to suggest to a patient or family that a lawyer is necessary?

A. Immediately after an adverse event.
B. When it is time to discuss compensation.
C. After your initial settlement offer has been refused.
D. Only when the patient or family asks about legal representation.

2. According to Richard C. Boothman, JD, chief risk officer and executive director of clinical safety at the University of Michigan Health System, what is one example of when it might be acceptable for a patient or family not to have legal representation after an adverse event?

A. When the patient is smart enough to say they don't want to give up one-third of their settlement to a lawyer.
B. When the settlement you offer is less than $25,000.
C. When the adverse event did not result in death.
D. When the adverse event involves a minor.

3. In the case involving comments made by anesthesiologist Tiffany M. Ingham, MD, during surgery, what part of the jury award does her employer have to pay?

A. $50,000 of the $200,000 in punitive damages
B. All of the $200,000 in punitive damages
C. $100,000 of the $200,000 in punitive damages
D. None of the punitive damages

4. With the Cardiac Children's Hospital Early Warning Scoring (C-CHEWS) scoring system, what would a score of 4 mean?

A. Green, meaning the patient is stable and the staff can continue routine care and scoring every four hours.
B. Yellow, prompting the staff to notify residents that the patient needs to be evaluated.
C. Mandatory activation of the rapid response team.
D. Automatic transfer to pediatric intensive care.

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Vendors can be the weak point in your HIPAA compliance efforts

You can't control business associates, but risk for your hospital remains

Business associates can frustrate compliance officers because they cannot be completely controlled, yet their performance can lead to a HIPAA breach for which the hospital or healthcare system is liable. Some providers are trying to use indemnification to escape that trap, but there are limitations to that strategy, too.

The best example of the threat is the 2011 breach at Stanford (CA) Hospital & Clinics, which was traced to a business associate's subcontractor, says **Marc Voses**, JD, a partner with the law firm Kaufman Dolowich & Voluck in New York City. A class action lawsuit against Stanford Hospital & Clinics and two business associates related to the breach affecting 20,000 patients was settled in 2014 for $4 million.

Court documents indicate that the breach occurred when a business associate's subcontractor posted information about 20,000 patients treated in the hospital's emergency department on a web site. The information was on the web site for more than a year before the breach was discovered.

The information about patients treated between March 1 and Aug. 31, 2009, included patient names, medical record numbers, hospital account numbers, emergency department admission/discharge dates, medical codes for the reasons for the visit, and billing charges, Stanford Hospital & Clinics confirmed at the time.

The case is indicative of the many ways that protected health information (PHI) is at risk once it leaves the healthcare company's data system, Voses says. He cites these most common security threats with vendors:

- lack of encryption of PHI at rest and in transit;
- use of portable storage media;
- sharing of information by vendor with non-business associates;
- improper disposal of written or electronic PHI;
- failure to maintain adequate security protocols and revise them periodically;
- use of cloud servers that are publically accessible.

Push for protection

The healthcare provider does have some leverage for requiring business associates to take proper HIPAA precautions, of course. Though these strategies have limitations, they should be pursued vigorously to obtain the most protection possible, Voses says. Those strategies include having a written agreement that outlines the terms of the relationship, requiring the vendor to retain a third party to verify the security protocols in place at the vendor and compliance with the said protocols, and requiring periodic audits of the vendor's systems that contain the provider's PHI.

Those strategies are increasingly difficult to implement when managing vendors and third-party risk across many industries, and with complex multi-vendor arrangements, notes **Bill Huber**, a managing director at Alsbridge, a global sourcing advisory and consulting firm based in Dallas. "This requires maintaining effective governance mechanisms to oversee the myriad touchpoints and linkages in the service delivery chain," Huber says. "The requirements of the healthcare industry, and of HIPAA specifically, mean that governance is especially critical."

Huber recommends these specific best practices for risk mitigation:

- appropriate due diligence on supplier information security controls and processes prior to selection and contracting of suppliers;

• specific contractual carve outs for HIPAA-related data breaches, with a separate, usually higher limitation of liability related to gross negligence or willful misconduct;

• specific notification requirements and audit rights in the contract related to information security controls and processes;

• mature vendor management processes and organization, including vendor risk management;

• transition readiness assessment (buyer and supplier) and testing prior to go-live/transfer of data;

• ongoing, periodic audits and tests of supplier controls;

• ongoing monitoring of supplier financial, regulatory, and legal alerts.

Pursue indemnification?

Because even the most diligent vendor compliance program cannot eliminate all potential liability from a HIPAA breach, some hospitals and health systems are pursuing indemnification, Voses notes. That strategy can reduce the risk and potential liability, but getting the vendor to agree to a meaningful indemnification agreement often is difficult, he says.

"It depends on the resources available to the vendor to indemnify you for a breach. When Target's breach was traced to an HVAC vendor, I doubt it could have paid for Target's losses," Voses says. The retailer estimates that about 42 million people had their credit or debit information stolen in 2013. Target settled a class action lawsuit for $10 million, according to court documents. "If the vendor has the resources, demand contractually provided liquidated damages for failure to protect PHI," Voses says. "Have the healthcare provider added to the business associate's cyber/data breach policy as an additional insured."

Unless you know the business associate would be unable to compensate you for the costs of a breach, start out by asking for every possible type of indemnification, advises **Jennifer Breuer**, JD, a partner with the law firm of Drinker Biddle in Chicago. That request should include any violation arising from the underlying business associate agreement or related to confidentiality and HIPAA compliance. But don't expect the vendor to sign off on that agreement.

"What business associates don't like about indemnification is that it completely changes the way they look at the underlying contracts and business associate agreement," Breuer says. "If the vendor is selling an item to the hospital for $12, they may look at the indemnification and realize they can't sell it to you for $12 if they might have to pay all the costs of a HIPAA breach."

When the vendor balks at a broad indemnification that leaves them on the hook for any breach in which the vendor is involved, the counter offer can restrict the indemnification so that the business associate is liable only when the breach is tied to specific actions for which it is directly responsible, she says.

"Reasonable people will agree that they have an obligation to have controls in place to protect PHI, and vendors are more likely to agree to indemnification when they see that it is tied to the actions that everyone in their industry is expected to do," Breuer says. "It is not unreasonable to ask for this type of indemnification, and it is not unreasonable to expect the vendor to agree to it."

The next issue

The next negotiating point involves whether the indemnification agreement will include a cap on the losses for which the vendor will reimburse the hospital or health system. A vendor with limited resources or doing a modest amount of business with the healthcare provider might want a cap so that a breach would not break the company or vastly outweigh the value of the hospital's business, Breuer explains.

"The cap could be the actual losses incurred by the hospital, or it could be related to the fees paid to the vendor," she says. "You might have an agreement that says the vendor's liability is limited to five times the fees paid to the vendor, for instance, so that the company can see the relative value of the indemnification. That emphasizes the point that you're not just trying to push off your legal problems on them, but rather that the hospital's business with that vendor comes with an obligation." ■

EXECUTIVE SUMMARY

Business associates must be monitored carefully to avoid HIPAA breaches that can pass on liability to the healthcare provider. Indemnity agreements can help mitigate the risk from breaches traced to vendors.

- Cloud servers and improper disposal of printed materials can cause breaches.
- Portable storage media are a common cause of breaches.
- Indemnification is a worthwhile option, even if only partial indemnification is possible.

CareFirst breach tied to Chinese attacks, limited by segmentation

Soon after CareFirst BlueCross BlueShield, based in Baltimore, MD, announced that the company had been the target of a sophisticated cyberattack, clues started arising to suggest that the same attack methods might have been used in this intrusion as with breaches at Anthem and Premera. Those incidents collectively involved data on more than 90 million Americans.

In those cyberattacks, security experts suspected the culprits were supported by China.

CareFirst announced that that the attackers gained limited, unauthorized access to a single CareFirst database. Approximately 1.1 million current and former CareFirst members and individuals who do business with CareFirst online who registered to use CareFirst's websites prior to June 20, 2014, were affected by the breach.

The breach was discovered as a part of the company's ongoing information technology (IT) security efforts in the wake of recent cyberattacks on health insurers. CareFirst engaged Alexandria, VA-based Mandiant, one of the world's leading cybersecurity firms, to conduct an end-to-end examination of its IT environment. This review included multiple, comprehensive scans of the CareFirst's IT systems for any evidence of a cyberattack.

The review determined that in June 2014, cyberattackers gained access to a single database in which CareFirst stores data that members and other individuals enter to access CareFirst's websites and online services. Mandiant completed its review and found no indication of any other prior or subsequent attack or evidence that other personal information was accessed, CareFirst reported.

The CareFirst attack suggests that hospitals and health systems are threatened by a much more challenging foe than the casual hacker. Security researchers at cybersecurity firm ThreatConnect in Arlington, VA, reported recently that the CareFirst attack has the hallmarks of the same scheme from China that was successful with other healthcare companies.

ThreatConnect explains the Chinese attacks in this way: Anthem was breached soon after a malware campaign that mimicked Anthem's domain names. Anthem was known as Wellpoint through 2014, and the ThreatConnect researchers found a series of subdomains for we11point.com (the "L's" in the domain were replaced by the numeral "1") — including myhr.we11point.com and hrsolutions.we11point.com.

ThreatConnect also found that the domains were registered in April 2014, when the Anthem database was breached. The domains were used with malware that masqueraded as a type of software commonly used to allow employees remote access to internal networks.

ThreatConnect reports that the same bulk registrant in China that registered phony Premera and Anthem domains in April 2014 also registered two CareFirst look-alike domains — careflrst.com (the "i" replaced with an "L") and caref1rst.com (the "i" replaced with the number "1"). ThreatConnect says the same tactics were used on EmpireB1ue.com (the "L" replaced with a number "1"). That domain was registered April 11, 2014, the same day as the phony CareFirst domains.

"It is believed that the prennera.com domain may have been impersonating the Healthcare provider Premera Blue Cross, where the attackers used the same character replacement technique by replacing the 'm' with two 'n' characters within the faux domain, the same technique that would be seen five months later with the we11point.com command and control infrastructure," ThreatConnect reported in a February 2015 blog post.

Re-evaluate data security

CareFirst reported that evidence suggests the attackers potentially could have acquired user names created by members to access CareFirst's website, as well as members' names, birthdates, email addresses, and subscriber identification numbers.

However, CareFirst user names must be used with a member-created password to gain access to underlying member data through CareFirst's website. The database in question did not include these passwords because they are fully encrypted and stored in a separate system as a safeguard against such attacks. The database accessed by attackers contained no members' Social Security numbers, medical claims, employment, credit card, or financial information.

"We deeply regret the concern this attack may cause," said CareFirst President and CEO **Chet Burrell**. "We are making sure those affected understand the extent of the attack — and what information was and was not affected. Even though the information in question would be of

limited use to an attacker, we want to protect our members from any potential use of their information and will be offering free credit monitoring and identity theft protection for those affected for two years."

The breach confirms a pattern of sophisticated attacks and should prompt compliance officers to re-evaluate their data security, says **Ken Westin**, senior security analyst with Tripwire, a software security firm in Portland, OR.

"Unfortunately, our predictions regarding the healthcare industry becoming a major target are being played out. Both insurance and provider organizations are becoming targets by criminal groups because the data stored on these systems has become more significantly valuable over time as criminal syndicates have found ways to monetize it," Westin says. "In general, healthcare organizations are not prepared for the level of sophistication associated with the attacks that will be coming at them. It's no surprise that several organizations have been targeted and compromised."

Try segmentation

One defense against the type of attacks attributed to China is segmentation of information, suggests **Marcin Kleczynski**, CEO of Malwarebytes, an anti-malware software provider in San Jose, CA. The strategy is that if you don't keep all your data in one place, you aren't likely to lose as much if one part of your system is breached.

"Segmentation of information is the name of the game in our modern threat landscape," he says. "Attackers are constantly increasing their ability to compromise secure networks, be it through new technologies or old-fashioned social engineering. If you treat a breach less like an 'it-won't-happen-to-me' scenario in favor of a stance that expects the breach to happen, you can help those who are charged with securing the information make a more effective battle plan."

CareFirst appears to have used segmentation successfully, Kleczynski says. One database was compromised, but it didn't include all information needed to access secure information, which limited its value.

"Think of the segmentation of secure information, such as login credentials, as the kind of safeguards a gun owner might employ," he says. "The gun is kept in one place and the bullets in another, both secured. In this case, the attackers were able to access the gun but were unable to find the bullets."

Kleczynski sees similarities with the computer breach at JPMorgan Chase in 2014, the largest intrusion of an American bank to date. Cyber attackers compromised information for 76 million households and seven million small businesses in the bank's databases. It took the bank's security team more than two months to detect and stop the intrusion. The Chase breach was similar in that, while the thieves managed to steal a large amount of data, the most valuable information was held in a deeper and more secure part of the network, Kleczynski says. This situation is similar to how a bank or museum would provide increased protection according to the relative value of different items, he notes.

"The CareFirst attack is proof that there are holes in the network that need to be fixed and also a sign that as a society we still have a lot to do in terms of making sure our personal information is kept secure," Kleczynski says. "At least we can find some solace in the fact that the bad guys were unable to get the juicy information."

Westin concurs and says that the cyberattackers are aware of the strengths and weaknesses of healthcare companies in the United States. Even if they are unlikely to get all the information they seek, they know that they still can access a substantial amount that has value. Also, they know that they can damage the company even without obtaining the most valuable information, he notes.

"As we saw with the recent tidal wave of retail breaches, attackers often take advantage of vulnerabilities that are endemic within an industry through common tools, frameworks, data storage/sharing methods or business processes," Westin says. ■

HIPAA breach attributed to stolen laptops

The latest HIPAA breaches across the country continue to reinforce the importance of basic security measures, with stolen laptops causing trouble for one hospital.

North Shore-Long Island Jewish (LIJ) Health System in Great Neck, NY, recently notified patients that their health information might have been compromised after laptops were stolen from a contractor's office. The health system determined that in September 2014, five laptops were stolen from the offices of Global Care Delivery, a firm based in Dallas that processes and collects payments from payers to hospitals. Data on about 18,000 North Shore-LIJ patients was on the four laptops. LIJ reported that the laptops were password-protected but not encrypted. ■

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

Failure to update a patient's EHRs leads to $35.4 million verdict against hospital

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 2004, a female Boston Marathon runner became dizzy after completing the race. The dizziness became so severe that the woman went to the hospital seeking treatment. The hospital administered an MRI and CAT scan, which revealed brain abnormalities in the patient. These brain abnormalities required her treating physician to put her condition into a central database to which her future physicians could have access. However, the physician who discovered the abnormality never put the information into the database.

Five years later, when the woman was pregnant, her obstetrician was not aware of the condition and recommended a natural birth. It is also worth noting that the patient never informed her obstetrician of the brain condition. Hours after the delivery of her baby, the patient had a massive stroke. The stroke left her completely paralyzed except for limited mobility of her right arm. The patient sued the first physician and the hospital where she worked for failing to enter her condition into the central database, which allegedly would have alerted her obstetrician of the condition and caused the obstetrician to order a cesarean birth that would have prevented the stroke. The defendants argued that the plaintiff should have informed her obstetrician of the condition. The jury agreed with the plaintiff and ordered the hospital to pay $35.4 million in damages.

... AN MRI AND CAT SCAN... REVEALED BRAIN ABNORMALITIES IN THE PATIENT ...

Background: Upon completion of the Boston Marathon in 2004, a female 25-year-old Pilates instructor became very dizzy. That same day, when the condition worsened, she went to the hospital. After explaining her symptoms of extreme dizziness brought on by the Marathon, the patient was given an MRI and CAT scan. These tests revealed that she suffered from a brain abnormality that is brought on by extreme stress, and she was released that same day. The patient later alleged that upon being released, she was made not made aware that high-stress activities, such as childbirth, could exacerbate her condition and cause complications.

The hospital where the patient initially was treated has a policy that requires the physicians to enter this type of information into a "Problem List," which is a version of the ever-developing electronic health records (EHRs). These EHRs are increasing in popularity and use, and the federal government and other institutions are working to develop national standards. Nevertheless, hospitals that sign on to use EHRs agree to input critical information such as a brain abnormality into the system. The EHRs then are viewed by other physicians to, among other things, help determine the best course of action for their patients. Unfortunately for the plaintiff, her information

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.

regarding the brain abnormality was neither added to the Problem List nor adequately documented in her medical records.

Four years later, at the age of 29, the woman became pregnant. Her obstetrician was never told about any brain abnormalities and searched the Problem List for his new patient. Having not seen her on the Problem List and with no other reason not to do so, the obstetrician recommended a natural childbirth. The obstetrician later contended that he would have ordered a cesarean if he was aware of the brain abnormality. Soon after the natural childbirth, the patient suffered a massive stroke. In addition to the stroke completely paralyzing her, with the exception of her right arm, the stroke required the patient to be in a medically induced coma for two months. An additional 16 months of hospitalization followed. Since that time, she has needed around-the-clock care and has lost the ability to communicate clearly.

The patient and her family sued the doctor and the hospital where she worked for failing to place her on the Problem List. They claimed that this failure put her at undue risk and eventually led to her life-altering stroke. The hospital, while sympathetic toward the plaintiff, argued that she should have informed the obstetrician of the condition.

The jury agreed that the physician and hospital not putting the plaintiff's brain abnormality on the Problem List was negligent and an undue risk. Furthermore, the fact that the plaintiff didn't appear on the list led to the obstetrician ordering a natural birth, which induced the extra stress that ultimately caused the patient's stroke and ensuing injuries. As such, the jury awarded the plaintiff and her family, which consists of herself, her husband, and their healthy daughter, $35.4 million in damages. The hospital, having failed to enforce its own policy and employing the physician, is responsible for the damages.

What this means to you: This case is revealing as to where the future of medical practice is headed and the high cost of not staying current with the changing field. In an ever-growing manner, the practice of medicine will further involve EHRs and similar databases that allow physicians to quickly access a patient's information.

While this news is excellent in terms of providing better healthcare, it could also be a source to which attorneys point when looking to impose legal liability onto a physician or hospital. The reason is that the fact of whether or not a patient's information is on any particular list is a clear and easily provable fact, and it almost certainly will be negligent not to add said patient's information into the EHRs when the hospital has agreed to do so.

With respect to EHRs, a successful plaintiff's attorney has suggested that something as minute as leaving one of the patient's allergies off of a database can lead to the patient's death or serious injury and a sizable legal penalty for the hospital that employs the physician who has fallen behind the times.

Given the trend of EHRs, adherence to these evolving standards and being sure to input the patient's information into the relevant EHRs is a must. Hospitals and physicians should be familiar with and embrace this digital change. Following the guidelines of the EHRs will result in providing existing and new patients better care as well as a means to protect the physician and hospital from costly medical malpractice litigation. As was specifically seen in this case, failing to adhere to the guidelines of the Problem List and input the brain abnormality into the database seven years prior — a task that would have presumably taken minutes — ended up leaving a patient paralyzed and costing the hospital more than $35 million in legal costs (and more than $40 million with interest). In any cost/benefit analysis, whether it be from a legal or medical practitioner, it is clear that adherence and enthusiasm toward the inevitable digital changes is the only path forward.

This case also shows the need for physicians to ensure they have elicited enough of their patients' relevant medical history to make an informed decision. While it is true that databases with this information are becoming more prevalent and that the obstetrician who was unaware of the plaintiff's brain abnormality did not face legal liability, a physician cannot solely rely on these databases or a cursory statement by the patient. A physician's failure to learn everything relevant about the plaintiff's medical history in this case led to a massive stroke and major health issues that the patient must endure for the remainder of her life.

Additionally, some in the legal community have suggested that the plaintiff or her obstetrician might be, at least partially, at fault for not having communicated about this issue themselves. As such, taking the time to explain the need for a complete medical history to the patient and ensuring the physician is aware of all relevant information can greatly benefit the patient and shield the physician and hospital from legal liability.

REFERENCE:

Norfolk County Superior Court, Mass. Case No. 14-1223 (May 7, 2015). ■

Decision not to operate on 2-year-old results in death and $6.25 million jury award

News: A 2-year-old girl died after her stomach ruptured from a recurring and treatable symptom. The girl had stomach issues in July 2009. After being sent to a second hospital, an examination of the gastrointestinal tract revealed the girl suffered from gastric volvulus, which can cause the stomach to twist on its axis. The condition naturally subsided, and the final diagnosis was gastroparesis, a condition that causes food not to properly pass through the stomach. The hospital staff released the patient the next day without following up on the girl's stomach, providing special care instructions, or informing the parents that surgery could prevent recurrence. The Discharge Summary that went to the family's primary pediatrician noted the stomach had fallen out of position. During two follow-up visits, the primary pediatrician treated the girl for constipation, told the parents the child didn't need a specialist, and told them to call the office if the condition worsened. On Oct. 25, 2009, the girl was exhibiting the same symptoms, which prompted the parents to call 911. They also called their pediatrician, who suggested the child didn't need to go to the emergency department (ED) but rather should stay home and be observed. The parents called off the ambulance. The next day, the girl's condition worsened. She was rushed to the ED, where she was pronounced dead two hours later. The cause of death was a rupture due to her stomach being out of place. The parents sued their primary pediatrician and the hospital where he worked, as well as the second hospital and its staff who failed to inform the parents of the need for surgery, perform the surgery, or complete the pre-surgery tests. Both hospitals maintained throughout the trial that the girl received proper medical treatment and this was a "one-in-a-million" occurrence. The jury found both hospitals negligent and responsible for the conduct of their staff members, including the pediatric surgeon and pediatrician. It awarded $6.25 million to the parents.

Background: In July 2009, a 2-year-old appeared to be nauseated. Her parents took her to a hospital, where she underwent an X-ray by recommendation of a physician who believed her stomach had distended. The X-ray revealed that her stomach was out of place, which is a form of gastric volvulus, and she was transferred to a second hospital for further tests. Further tests ruled out many possible causes, but a review of the gastrointestinal tract results confirmed the girl's stomach was out of place. The reviewing physician called the findings "critical," believed surgery could be necessary to hold the stomach in place, and consulted with the hospital's pediatric surgeon. The pediatric surgeon was unsure if the 2-year-old should be operated on and ordered a CT scan. The pediatric surgeon and treating physician conferred about the upcoming CT scan, but the pain and other symptoms the girl was experiencing had subsided. The treating physician gave the girl a physical examination and determined the cause of the symptoms was gastroparesis. The treating physician placed her on clear liquids and sent her to another room for observation. After seeing that the nutritional therapy was improving the girl's condition, she was released from the hospital without receiving a CT scan or the surgery. The girl's Discharge Summary noted that the "upper GI suggested organ axial rotation of stomach and small bowel malrotation" but concluded the girl was experiencing gastroparesis as the final diagnosis. Aside from being told to follow up with their pediatrician, the girl's parents later alleged that they were not given special discharge instructions regarding the possibility their daughter's stomach could "twist" again or that surgery could correct the condition.

The girl followed up with her primary pediatrician twice in the following months. Her primary pediatrician treated her for the gastroparesis and never mentioned anything to her parents regarding the stomach being out of place, information which was in the Discharge Summary report the pediatrician is alleged to have received. When asked by the girl's mother whether there was a need to see a specialist for the 2-year-old's stomach condition, the pediatrician informed her there was no need but to call the office if her condition worsened.

On Oct. 25, 2009, the girl's parents called 911 because she was exhibiting intense abdominal pain. The parents also called the girl's primary pediatrician, who recommended that the parents not take her to the ED but observe her instead. The parents, who later said they were acting on their pediatrician's advice, canceled the ambulance that was on its way.

The next day, while still at the

family's home, the girl was vomiting and unable to drink anything. Her parents called 911, and she was rushed to the ED. Just more than two hours after arriving, she was pronounced dead. An autopsy ruled the cause of death was her stomach twisting, which caused it to rupture.

The girl's parents sued the second hospital and its staff. The lawsuit included the pediatric surgeon for not recommending surgery, her treating physician who released the girl without recommending or explaining the need for surgery, and the hospital for the acts of its employees and for not following protocol. They also named her primary pediatrician and the hospital where he worked for failing to be aware of the severity of the patient's condition and for not recommending she see a specialist for the stomach abnormalities or go to the ED the day before the girl died.

The defendants maintained that they followed proper protocol and didn't commit negligence or medical malpractice. The jury found the staffs of both hospitals acted negligently for not informing the parents that the surgery to correct the gastric volvulus could have prevented the stomach from twisting again. The jury awarded the parents $6.25 million in damages.

The damages breakdown was $3.7 million for wrongful death, $2.5 million for future loss of earnings and earning capacity, and $50,000 for pain and suffering. The pediatric surgeon was found 65% liable of the damages, the treating physician was found liable for 10% of the damages, and the hospital where these physicians were working was found liable for 5% of the damages. The family's primary pediatrician was found liable for 20% of the damages.

What this means to you: This case displays the need for physicians to consult, consider, and acknowledge the suggestions and recommendations of other physicians in general, and especially at the hospitals where they work. In this situation, the pediatric surgeon knew the prior testing revealed "malrotation" of the stomach. The doctor who initially reviewed the findings of the test considered this "critical" and recommended surgery. However, the severity of the prior findings and recommendation of surgery by the reviewing physician were not conveyed in the report of the pediatric surgeon to the treating physician who released the girl.

When her symptoms subsided and a physical exam suggested the problem was gastroparesis, the physician likely felt comfortable releasing her without further inquiry. Yet, if the report by the pediatric surgeon emphasized the need for surgery as much as the report given to him did, the girl likely would not have been released without the completion of pre-surgery testing and an explanation to the parents regarding the possible necessity of surgery. Thorough reporting of all the physicians' suggestions, following through on the suggestion for pre-surgery tests, or explaining the need for surgery to the girl's parents would have served to shield the hospital from liability. All are based on communications with other physicians and the patient. A physician should take special care to accurately convey to the next physician all potentially relevant and known information and opinions, and the physicians should be equally as diligent in explaining those findings to their patients and their patients' parents.

Another lesson is that a primary care physician should thoroughly examine the Discharge Summary by the physician at the hospital from which the patient came. Here, the Discharge Summary noted that the girl's stomach had been out of position. However, her primary pediatrician didn't recommend the girl seek further treatment, but he treated the child for constipation. Had the malrotation of the stomach been fresh in the primary physician's mind, further treatment or consultation might have been recommended when the mother initially asked.

Lastly, a physician should call off emergency services only if he or she is certain it is the right decision. When a patient is being rushed to the hospital by ambulance for conditions similar to the ones a physician believes he or she has treated, that physician should not assume it is for the exact same condition. Preventing a patient from receiving care, which is later shown to be have been necessary, can clearly harm the patient and will rarely be perceived favorably by a jury.

Also, a physician shouldn't prevent a patient from seeking aid from another physician, hospital, or emergency aid service without first conducting a physical examination. The parents halted the emergency services that could have saved her life, and they followed the suggestion of their pediatrician who likely assumed the condition was the same constipation issue that would pass. A physical exam or thorough review of the file would have revealed the malrotation of the stomach months prior. It likely would have led to the ambulance trip and the girl receiving life-saving aid. Physicians must be certain when preventing a patient from receiving emergency aid or care from another physician.

REFERENCE:

Court of Common Pleas of Pennsylvania, Luzerne County. Case No. 11-09921 (May 20, 2015). ■