35th Anniversary

Healthcare RISK MANAGEMENT

May 2014 | Vol. 36, No. 5

Pages 49 - 60

Health system sued by doctor who was fired for Facebook post

ED physician posted comment about patient, used initials

Social media is again creating problems in healthcare, this time with an emergency physician who was fired for making a comment on Facebook about a patient after a nurse posted a picture of the woman's buttocks. The health system promptly dismissed the contract physician, but she is now suing.

Catherine Puetz, MD, the former associate medical director of emergency services with Spectrum Health Hospitals in Grand Rapids, MI, was dismissed because of a comment she posted on Facebook. She was responding to a picture of a patient's bottom on Facebook that was posted by an emergency department (ED) nurse. *(See the story on p. 40 for more details on the incident.)*

The lawsuit says President **Kevin Splaine** accused Puetz of "reprehensible behavior" and "a lack of integrity." The president told her the Facebook comment violated the Health Insurance Portability and Accountability Act (HIPAA) and that justified her dismissal, according to the lawsuit. Puetz contends in her lawsuit that the comment did not violate HIPAA and that Spectrum used the incident as an excuse to fire her because the two parties had disagreed over the copyright of materials she developed for evaluating patients in observational units. Spectrum claimed that it controlled any materials developed while Puetz worked at the hospital and could deny the doctor's plans to use them in consulting with other facilities.

The health system promptly dismissed the contract physician, but she is now suing.

The lawsuit accuses Spectrum of defamation and breach of contract and seeks at least $75,000 from Spectrum Health, Splaine and Vice President Jeanne Roode, in addition to unspecified punitive damages. Puetz also is asking the court to declare that Puetz owns the copyright on materials developed for observation units.

Easy to cross the lines

The case illustrates how pervasive social media have become and how easily a hos-

INSIDE

AHC Media

www.ahcmedia.com

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.

pital representative can cross the lines, says **Jason Koors**, JD, legal counsel with MemorialCare Health System in Fountain Valley, CA. The nurse who took the photo and posted it put herself and the hospital at risk for liability in a civil lawsuit, he notes. So far there has been no mention of lawsuits, but Koors says that is almost inevitable now that the incident has been made public.

'Incredibly inappropriate'

Koors has no doubt that the physician and nurses should have known their actions were wrong. *(See the story on p. 40 for questions about the chief medical officer's actions.)*

"If the subject of the photo was a Spectrum Health patient, then the Facebook post is likely a HIPAA violation," he says. "But at the very least, it is incredibly inappropriate. I would not be surprised if the ED nurse who posted the photo was terminated, especially if she was at-will. Such careless disregard for patient privacy likely violated the health center's policies or code of conduct. As an MD, Puetz should have known better than to comment on the photo and add more potentially identifiable information. I think it is grounds for terminating her contract."

The doctor's post included the patient's initials, which elevates the doctor's actions to a more serious offense and clearly a HIPAA violation, says **Philip Becnel**, managing partner of Dinolt Becnel & Wells Investigative Group in Arlington, VA. A private investigator who handles many healthcare cases, Becnel says the people might underestimate how much one can learn from just two initials. He and his fellow investigators often rely on small bits of data such as initials to track down individuals.

"The logic of firing the physician but not the nurse who made a comment makes sense to me," he says. "Saying you like big butts or whatever ridiculous comment that was doesn't add any information to the situation, but the doctor added potential identifiers when she included the patient's initials. The other comment was arguably more inappropriate, but it didn't constitute a HIPAA violation." *(See the story on p. 41 for more on using social media as a legal defense.)*

Likely a HIPAA violation

Puetz's lawsuit contends that Spectrum overstated the offense by declaring it a HIPAA violation, but others don't see it that way. For a HIPAA

Executive Summary

An emergency physician is suing Spectrum Health for firing her after a post on Facebook. The post involved a patient who had been treated at the facility.
- ✦ An emergency department nurse originally posted a photo of a patient's buttocks that drew the physician's comment.
- ✦ The physician's use of the patient's initials might have violated privacy rules.
- ✦ Monitoring social media can provide a defense for wrongful termination.

Healthcare Risk Management® (ISSN 1081-6534), including HRM Legal Review & Commentary™, is published monthly by AHC Media, LLC, 950 East Paces Ferry NE, Suite 2850 Atlanta, GA 30326. Telephone: (404) 262-7436. Periodicals Postage Paid at Atlanta, GA 30304 and at additional mailing offices.

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

AHC Media, LLC is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation. This activity has been approved for 15 nursing contact hours using a 60-minute contact hour.

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

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

Healthcare Risk Management® is intended for risk managers, health system administrators, and health care legal counsel. Opinions expressed are not necessarily those of this publication. Mention of products or services does not constitute endorsement. Clinical, legal, tax, and other comments are offered for general guidance only; professional counsel should be sought for specific situations.

Executive Editor: **Joy Daughtery Dickinson** (404) 262-5410 (joy.dickinson@ahcmedia.com). Production Editor: **Kristen Ramsey.** Director of Continuing Education and Editorial: **Lee Landenberger.**

SUBSCRIBER INFORMATION

Customer Service: (800) 688-2421 or fax (800) 284-3291, (customerservice@ahcmedia.com). Hours of operation: 8:30 a.m.-6 p.m. Monday-Thursday; 8:30 a.m.-4:30 p.m. Friday.

Subscription rates: U.S.A., **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. 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.)

violation, the doctor must have shared information about a patient that was protected, in an identifiable manner, and for reasons other than what is allowed under HIPAA, explains **R. Stephen Trosty**, JD, MHA, CPHRM, president of Risk Management Consulting in Haslett, MI, and a past president of the American Society for Healthcare Risk Management (ASHRM).

"It seems obvious that the sharing was not for protected purposes. It also seems to me that the provided information might enable people to identify the patient. Therefore, it seems to me that we have a HIPAA violation," he says. "I would argue that sharing on Facebook is, in theory, no different than sharing in a local newspaper or through word of mouth. It is a mechanism whereby others who read or hear the information can identify a patient who was in the hospital and was not for a protected purpose."

HIPAA requires strong response

Remember: The HIPAA violation penalty would be against the hospital, and hospitals are required to enforce their own policies regarding patient privacy, Trosty says. The hospital also must show that it takes appropriate action in response to a HIPAA violation, and this action often includes dismissal, he says.

The appropriateness of the penalty depends in part on what policies the hospital had in place before the incident, Trosty says. If there was a policy clearly prohibiting such comments, the severe punishment of dismissal is more easily justified. If not, the lack of such a policy raises issues not only about the appropriateness of the punishment but also about HIPAA compliance by the hospital, he says. Physician training in HIPAA policies also should be questioned. Was there a requirement in the contract the doctor had with the emergency department group for HIPAA training? Did the hospital require such a clause in the contract between the doctors and the emergency department group?

If the answer is yes and the doctor attended, the punishment is justified because she violated rules taught in the training, Trosty says. Even if it was a requirement and she did not attend, the punishment might stand, he says. Trosty emphasizes that Spectrum was risking severe penalties if it did not respond in a way that the federal government would consider sufficiently aggressive.

"I think it has to be recognized that the federal government is being even stricter when it comes to HIPAA compliance, enforcement, and training by hospitals and to appropriate action taken for violation," he says. "I do think this should be considered when you're looking at whether dismissal was justified."

Regrettable social media posts are not always HIPAA violations or even an actionable offense by an employee, Koors notes. For example, Section 7 of the National Labor Relations Act (governing union and non-union employees) gives employees the right to engage in protected concerted activities for the purpose of collective bargaining. Recently, this statutory right has been extended to protect Facebook posts in which employees comment on the conditions of their employment, such as discussing wages, complaining about management, and criticizing working conditions, he explains. The Spectrum Health incident probably would not be covered by Section 7, Koors says, because the photo did not touch on conditions of employment. And even if Section 7 did apply to the post, the protection might not protect Puetz's comment because she is a contractor rather than an employee.

Guidance questioned

The health system probably should have taken more time to consider its response, suggests says **Jane McCaffrey**, DFASHRM, MHSA, director of compliance and risk management at The Blood Connection in Greenville, SC, and a past president of ASHRM. Less than a month passed before Spectrum dismissed the doctor.

Healthcare providers should have a social media policy now because the risk of privacy breaches is higher than ever before, partly because such a large percentage of employees use social media, and their familiarity can lead to a casual approach, McCaffrey says. *(For more on social media risks, see* Healthcare Risk Management*, March 2012, pp. 25-30.)* She also notes that the chief medical officer (CMO) comment might indicate a lack of guidance from administration.

"When there is a suspected violation by employed or contracted personnel, there should be a systematic evaluation that goes beyond the CMO providing what sounds like informal feedback," she says.

Was the compliance office or privacy officer involved in the incident, and was the doctor properly trained in HIPAA compliance, asks **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 ASHRM?

Rather than posting a comment when Puetz saw the post, she should have personally contacted the nurse who made the post and advised it be taken down and explained why, Kicklighter says. "The next step is to make a report to the hospital compliance officer to take any next steps necessary," she said.

SOURCES

- Philip Becnel, Managing Partner, Dinolt Becnel & Wells Investigative Group, Arlington, VA. Telephone: (202) 638-5000. Email: becnel@dinolt.com.
- Leilani Kicklighter, RN, ARM, MBA, CPHRM, LHRM, The Kicklighter Group, Tamarac, FL. Telephone: (954) 294-8821. Email: lkicklighter@kickrisk.net.
- Jane McCaffrey, DFASHRM, MHSA, Director of Compliance and Risk Management, The Blood Connection, Greenville, SC. Telephone: (864) 751-3092. Email: jjmccaffrey49@gmail.com.
- Jason Koors, JD, Counsel, MemorialCare Health System, Fountain Valley, CA. Telephone: (714) 377-3243. E-mail: jkoors@memorialcare.org.
- R. Stephen Trosty, JD, MHA, CPHRM, President, Risk Management Consulting, Haslett, MI. Telephone: (517) 339-4972. E-mail: strosty@comcast.net. ✦

Buttocks photo, patient initials lead to doctor's dismissal

The lawsuit against Spectrum Health in Grand Rapids, MI, filed by **Catherine Puetz**, MD, outlines the incident that led to her dismissal. This is a summary:

The incident occurred on Aug. 5, 2013, when the former associate medical director of emergency services saw a picture of a patient's bottom on Facebook that was posted by an emergency department nurse. Puetz thought she recognized the woman's buttocks as belonging to someone she had seen in the ED and also outside of the hospital. She posted a comment to the photo that read "OMG. Is that TB?"

A nurse also posted a comment to the photo that read "I like big butts and I cannot lie…," a line from a song by Sir Mix-a-Lot. When the exchange was reported to hospital officials soon after, Spectrum Health investigated and took "appropriate action," according to a statement released by the hospital. Puetz, an employee of Emergency Care Specialists, an independent contractor that provides emergency department staff to Spectrum Health, was fired. The nurse that quoted the song lyric was reprimanded. It is not clear how Spectrum disciplined the nurse who posted the photo. Spectrum Health declined to comment and Puetz's attorney could not be reached.

Puetz recently filed a lawsuit in U.S. District Court against Spectrum Health Hospitals, President Kevin Splaine and Vice President Jeanne Roode.

In her lawsuit, Puetz contends that she submitted an apology to the nursing director and was assured by the chief medical officer that her job was not on the line. Nine days after the posting, however, Puetz was notified that she was being dismissed as associate medical director in emergency services but could continue to work as an emergency physician. Five days after that, she was told that she could not practice medicine at any Spectrum Health facility. ✦

CMO's statement could complicate hospital's defense

The alleged claim by a fired emergency physician, that the chief medical officer (CMO) assured her that her job was not in jeopardy, could complicate matters for the hospital, which is being sued by the doctor, says **Jason Koors**, JD, legal counsel with MemorialCare Health System in Fountain Valley, CA.

Spectrum Health in Grand Rapids, MI, dismissed the doctor after she posted a comment on Facebook in response to a nurse posting a photo of a patient's buttocks.

"Whenever conducting an investigation, human resources should always advise senior management against making promises to employees or offering assurances of job security," Koors says. "It's all about managing expectations."

The CMO's action also concerns R. **Stephen Trosty**, JD, MHA, CPHRM, president of Risk Management Consulting in Haslett, MI, and a past president of the American Society for Healthcare Risk Management (ASHRM). The repercussions of an assurance that the doctor would not be dismissed might lie in a court determination of whether the CMO acted as an agent of hospital and had the authority to do so. If the CMO was overstepping, the statement to Puetz carries no weight, Trosty says. If the CMO was properly acting as an agent, the statement probably would prevent dismissal but not some lesser punitive action, he says.

"If the CMO had the authority to act as the hospital's agent and made the statement, it would not preclude taking some type of action since I do not believe any hospital personnel, including the CEO, can do this if it would result in a penalty to the hospital for failing to properly respond to a HIPAA violation," Trosty explains. "The hospital is expected to take some action for violation, but I do believe this might be a gray area that could require some form of judicial determination. It also becomes an issue for the hospital, as a separate concern, to deal with the CMO if he or she exceeded existing authority when making the statement."

Medical staff bylaws or hospital policy should spell out who has ability to make these types of statements that a hospital might have to live with later, he says. ✦

Dig into social media as defense to dismissal lawsuits

Healthcare providers should use social media research as a defense tool when sued by employees and physicians, says **Philip Becnel**, managing partner of Dinolt Becnel & Wells Investigative Group in Arlington, VA. A private investigator, Becnel handles many healthcare cases, which involves interviewing employees about their work situations and conducting background checks into their social media postings.

"It's how people communicate now, and a good percentage of our cases have a social media component," he says. "It's sort of standard now in the defense attorney's playbook to request the records of those communications. The first thing we do now is get their identification and download every single tweet and post on their accounts. There's a lot of evidence out there just for the taking."

Even without a lawsuit, healthcare providers would benefit from monitoring social media, Becnel says. Posts might not violate HIPAA or other restrictions, but they still can be useful in alerting administrators of policy violations, a growing unease among employees, or potentially unsafe practices. Having a strong social media policy will provide a basis for investigating an individual's posts and also justify punitive action, he notes.

"If you don't have a good policy, and the employee does something to hurt the employer, you don't really have any right to investigate that person's social media without first notifying the employee," Becnel explains. "Once you notify them, they can delete the content and stymie the investigation."

Social media posts also can be used to show that an employee was unhappy in the job for some time before being dismissed. That record of unhappiness can help defend against claims that the employee was unfairly forced out of the job, Becnel says.

"The employer can go back and show that he was unhappy with his job for a year before this incident, and that was the real reason you quit, not because of this one incident where you say we treated you unfairly," he says. ✦

State laws can affect your whistleblower response

Some states limit how aggressive you can be

Healthcare providers are facing more whistleblowers than ever before, as employees and others realize they can reap big rewards from exposing fraud. A strong and coordinated response is necessary, but exactly what you can and can't do is dictated by state laws that can vary substantially.

Providers must tread carefully when faced with potential whistleblower claims, says **Alex J. Brackett**, JD, partner with the law firm of McGuireWoods in Richmond, VA. State legislatures have taken different approaches to protecting whistleblowers and the organizations accused, so you must know your own state law, he says. Those laws also are changing.

For instance, whistleblowers in California benefited from new laws that took effect Jan. 1, 2014. The laws expanded whistleblower protections in the state. The new statutes modified existing whistleblower protections in California, which already were considered among the most protective. Under the new statutes, employees are encouraged to identify potentially illegal activity without fear of retaliation.

Whistleblowers in California are now protected from retaliation for reporting suspected activity internally, as well as externally. The law includes internal auditors. Definitions of prohibited retaliation were expanded to include anticipatory retaliation against a potential or suspected whistleblower.

New Jersey took a different tack, with an appeals court ruling in December 2013 that states whistleblower protections did not apply to an employee charged criminally for taking confidential documents related to the alleged wrongdoing. In State v. Saavedra, a Board of Education clerk had filed a complaint against her employer alleging retaliation for her reporting pay irregularities. To support her case, she provided her attorney with confidential documents. The county prosecutor obtained an indictment for theft.

The defendant sought to dismiss the indictment and cited an earlier ruling that an employer could not terminate an employee for the unauthorized taking of documents to support an employment discrimination case. The appeals court agreed with the trial court that this ruling did not extend to criminal cases, and the court said it had serious concerns about supplanting the judicially supervised discovery process in discrimination claims.

"Every state is going to have its own whistleblower protections, and the variance could involve any number of things," Brackett says. "In many cases they define specific types of people or specific topics that can qualify for protection under the whistleblower laws. A state might have very narrowly defined categories and in others it can be very broad."

Default to most restrictive laws

The issue is complicated when a healthcare organization has facilities in several states. Researching each state law and formulating appropriate policies can be time-consuming, so Brackett says some providers determine which of their locales has the broadest definitions and the most protection for whistleblowers, and then they build their systemwide whistleblower policy on those.

"If you are acting as if that restrictive set of parameters applies, then you're covering your bases everywhere," Brackett says. "You will be handling yourself in a way that satisfies everyone. If a state has some sort of outlier definition or requirement that is really odd, you can have just a minimum of rules that cover that in addition to your blanket policy."

However, once you have a whistleblower incident, it can be wise to dig deeper into that state's applicable laws, he says. In this way you avoid spending time and money on researching each state's laws and writing separate policies, but once a claim is made you can take advantage of what the state allows and double-check that you are not violating any state-specific limitations.

"That's where the problems usually occur, not in the day-to-day operations, but in the response to a whistleblower," Brackett says. "That's when you can get allegations of retaliation or changing someone's work assignment as a way that can be construed as retaliatory. As long as your managers have been trained well in a whistleblower situation, then you typically will be in a good position to investigate the claims and come to a resolution."

Brackett notes, however, that there is some risk in creating an organization-wide policy that is the most conservative so that it complies with the law in all your applicable states, and then upon further research taking more aggressive action that is allowed under the one state's laws in a particular incident. The other party could question why you took action that is not consistent with your own policy.

"That is always a potential trap if the other side can show your policy and ask why you didn't follow it," he notes. "In this case, you can explain that you were acting in the most conservative manner across the board, but then followed the specific state laws that apply to an actual situation. There is some risk/reward balance in taking this approach."

Executive Summary

State laws can vary significantly regarding a provider's options when responding to a whistleblower. Risk managers should study their own state laws to know the limits and opportunities.

- ✦ California recently passed laws giving providers more freedom to respond to whistleblowers, but New Jersey passed more restrictive legislation.
- ✦ The differences can affect what constitutes prohibited retaliation.
- ✦ Some laws are written to encourage more internal reporting rather than whistleblowing.

SOURCE

• **Alex J. Brackett**, JD, Partner, McGuireWoods, Richmond, VA. Telephone: (804) 775-4749. Email: abrackett@mcguirewoods.com. ✦

Huddles getting popular, but use them correctly

Risk managers and clinicians are finding that huddles are an effective way to improve patient safety and identify deficiencies, but there is little guidance on how to conduct them. Experienced huddlers say a formal plan for the huddle will yield more valuable results.

A huddle is a gathering of involved and interested personnel soon after a patient safety event to discuss what happened, why it happened and how the problem might be prevented. They have been used for all manner of patient safety issues, and Nationwide Children's Hospital (NCH) in Columbus, OH, has found them to be especially effective with medication events, says **Shelly Morvay**, PharmD, medication safety pharmacist at the hospital.

Huddles helped decrease the absolute number of harmful adverse drug events (ADEs) by 74%, and the ADE rate per 1,000 dispensed doses decreased by 85%, Morvay says. ADEs are defined as injuries resulting from medical care involving medication use.

NCH has conducted more than 800 medication event huddles over three years

Executive Summary

Huddles are used by many providers to improve safety, but there are few guides for how to conduct them. A specific format will improve the results of the huddle.

- ✦ Conduct the huddle soon after the event.
- ✦ Have a specific format that is used for all huddles.
- ✦ One hospital reports using huddles to reduce harmful adverse drug events by 74%.

and identified more than 3,000 improvements. ADEs accounted for approximately two-thirds of reported patient harm at NCH.

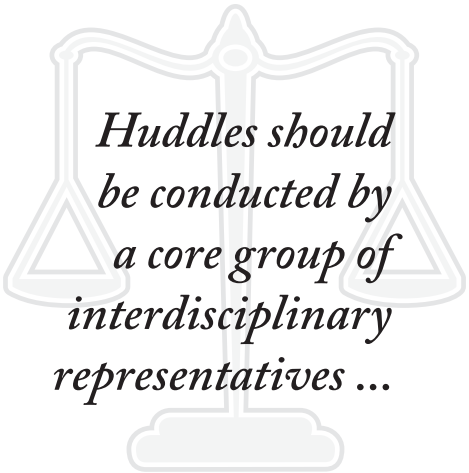
The quick-investigation huddle tool was proposed as a means to engage frontline staff in identifying process improvements that might contribute to ADE elimination, Morvay says. In March 2010, NCH piloted the medication event huddle process in its critical care units, and in 2011, it introduced the process to all inpatient units and some ambulatory clinics. Subsequently, NCH has spread the process to ADEs that occur anywhere in the organization, including all ambulatory clinics, the emergency department, perioperative areas, and interventional radiology.

NCH's success with the huddles yielded some information about what makes them productive. Responding the ADE quickly was a prime concern; the 30-minute medication event huddles were initiated and scheduled within 24 hours whenever an ADE was identified. The essential components of the huddle included:

- an explanation by the core huddle team leader of the huddle process;
- simulation of the ADE using the actual electronic medical record, infusion pump, pharmacy labels, and other equipment or supplies;
- review of a standard list of questions to identify environmental or practice factors that may have contributed;
- assignment of identified interventions or "tests of change" to appropriate participants;
- follow-up communication about "tests of change" via email;
- encouragement to speak with colleagues about the specific ADE and huddle experience.

In addition, the medication event huddles were used as an opportunity to promote a culture of safety, increase involvement of frontline staff, and speed improvement efforts, says Clinical Coordinator **Dorcas Lewe**, RN, MS, who worked closely with Morvay on the huddles. Morvay and Lewe estimate that medication event huddles require a minimum of 0.5 full-time equivalent (FTE) nurses to review the ADEs, schedule the huddles, and follow up on completion of recommendations. While huddles do not replace a formal root cause analysis (RCA) or daily safety walkarounds by leaders, they do enable a more rapid identification of the cause and subsequent intervention, they say.

Huddles should be conducted by a core group of interdisciplinary representatives, Morvay says. The other people in the huddle should include frontline staff who were involved with the incident or are familiar with it, along with unit leaders. Staff members are reminded that the huddle is a brainstorming session and not intended to single out any person as responsible for the event.



"We encourage them to be honest about what they think occurred," Lewe says. "They are always informed about the huddles by their managers so that it is coming from someone they know. It's not a call from administration."

Managers know that they are free to forward the huddle invitation to anyone else that might contribute useful information, Lewe says. After the brainstorming in the huddle, any necessary interventions are assigned to specific huddle attendees.

Huddles empower staff

Risk manager **Carol McGlone**, RN, says the huddles have become a valuable asset in the hospital's overall patient safety program. One of the benefits is that huddles produce useful information much faster than a full RCA, which comes later.

"We have seen over time that staff will report an incident or a near-miss and suggest a huddle is appropriate, rather than waiting for leadership to call a huddle. This is true of events that do not involve medication safety, so that tells me that the staff see the value of huddles and appreciate the opportunity to give input," McGlone says.

McGlone participates in some huddles at NCH, collaborating closely with the quality improvement department and clinical leaders.

NCH conducts medication safety huddles once or twice per weekday, as warranted, Lewe says. The hospital uses certain criteria to determine when a huddle is appropriate, but staff members are free to request a huddle even when those criteria are not met, she says. The criteria for calling a huddle include the need for intervention or additional monitoring, severity of an event, and incidents involving high alert medications or specific focus areas such as medication reconciliation. A huddle also is called when there is a misstep or near-miss when implementing a new policy.

A summary of the information gleaned from the huddle is shared through Microsoft's Sharepoint software to everyone who attended the huddle and those who were invited but could not come. Any huddle attendee who was assigned an intervention also receives a recap of the action needed and when it should be completed, along with frequent reminders until it is done.

The huddle soon will be implemented in the hospital's employee safety program, McGlone says.

At South Nassau Communities Hospital in Oceanside, NY, huddles are used routinely for everything from planning the day on a unit to serious adverse events, says **Ruth Ragusa**, RN, vice president of organizational effectiveness. She has found that the timing for a huddle must be tailored to the individual event. Some should be held as soon as possible, before people for-

get the important details, while others might be delayed for a day.

"With some incidents, the staff are still dealing with it, and you can't pull them away from patient care," she says. "We also try to let the staff diffuse their feelings about it, because sometimes it can be upsetting to them and they need a breather before you ask them to recount the incident."

SOURCES

• **Dorcas Lewe**, RN, MS, Clinical Coordinator, Nationwide Children's Hospital, Columbus, OH. Telephone: (614) 722-5066. Email: dorcas.lewe@nationwidechildrens.org.

• **Carol McGlone**, RN, Risk Manager, Nationwide Children's Hospital, Columbus, OH. Telephone: (614) 722-3946. Email: jodi.mascolino@nationwidechildrens.org.

• **Shelly Morvay**, PharmD, Medication Safety Pharmacist, Nationwide Children's Hospital, Columbus, OH. Telephone: (614) 722-2185. Email: shelly.morvay@nationwidechildrens.org.

• **Ruth Ragusa**, RN, Vice President of Organizational Effectiveness, South Nassau Communities Hospital, Oceanside, NY. Telephone: (516) 632-3999. Email: rragusa@snch.org. ✦

Interventions reduce serious events 83% at one hospital

A five-year effort to improve quality has resulted in an 83% reduction in serious safety events at Vidant Health in Greenville, SC, along with several other achievements.

During the last five years, Vidant Health has outlined interventions to improve patient safety and quality that included board literacy in quality, an aggressive transparency policy, patient-family partnerships, and leader and physician engagement. Implementation of specific tactics associated with each approach occurred in the ensuing years, explains **Joan D. Wynn**, PhD, RN, CPHQ, chief quality officer with Vidant Health in Greenville, SC, which has nine hospitals, 70 physician practices, and ambulatory surgery and home health/hospice services.

Other achievements include a 62% reduction in hospital-acquired infections, a 98% optimal care in core measures from the Centers for Medicare and Medicaid Services (CMS), patient satisfaction ratings above 80%, and more than 150 patient advisors partnering with leaders, physicians, and front-line staff in safety and quality work.

A first step in the transformation was to ensure that the Vidant board of directors understood their fiduciary responsibility for overseeing quality in the system, Wynn says. To improve the board's quality literacy, Vidant sent the board members on retreats, brought in quarterly speakers, and conducted educational sessions.

"We wanted them to know the questions they should be asking when we present the quality data," Wynn says. "They needed to learn to read the quality scores also. That way the board could drive the improvement and make sure we were hitting this effort throughout the system."

To improve the transparency of quality measures, Vidant developed a standard quality score card that is used in the same way across all venues from the bedside to the boardroom, Wynn says. Color-coded measures helped everyone quickly seize the meaning of the data.

"We also wanted to make that information transparent beyond our organization, so if you go to the website for any of our hospitals, you will find easy-to-understand data on compliance with best practices like handwashing and infection prevention, and also outcome data on the numbers of infections and falls," Wynn says. "That helped spur us to do our best, because we knew that data was going to be public, and we wanted it to be as good as possible."

Patient and family partnerships also were important in improving patient safety and quality. Each hospital has a position called the patient care advisor, non-healthcare professionals who sit on many key committees and provide guidance from a patient's perspective.

"That involvement facilitates having patients tell their stories to our leadership team, to the board, and to employees," Wynn explains. "We have had patients or family members describe their experiences in our organization, and that is a very compelling way to engage the hearts and minds of our employees to keep them working on continuous quality improve-

Executive Summary

A health system has reduced serious adverse events by 83% over five years. The improvement is the result of a system-wide quality improvement effort.

✦ Hospital-acquired infections were reduced 62%.

✦ The system achieved a 98% score in core measures from the Centers for Medicare and Medicaid services.

✦ Patients can show the board of directors the impact of quality initiatives.

ment. Putting a face to the numbers on the quality score card really helps."

The first patient to tell her story to the Vidant board had suffered a surgical complication that led to an infection, eventually spending 90 days in the hospital.

"She told the board, 'when you look at those quality score cards, I'm one of those ventilator pneumonias you see there,'" Wynn recalls. "Putting a face to the data, reminding them that it is people and not just data, definitely had an impact."

SOURCE

• **Joan D. Wynn**, PhD, RN, CPHQ, Chief Quality Officer, Vidant Health, Greenville, SC. Telephone: (252) 847-1946. Email: jwynn@vidanthealth.com. ✦

Stanford, contractor to pay $4.1 million over privacy

It will take $4.1 million for Stanford (CA) Hospital & Clinics and one of its former contractors to settle a class action lawsuit claiming the hospital violated state privacy law by allowing the protected health information (PHI) of 20,000 emergency department patients to be posted online for nearly a year. The PHI was found on a website that helped students answer homework questions.

Shana Springer sued the hospital and Los Angeles-based Multi-Specialty Collection Services in 2011 and said her information was part of the information found on the site. She was one of the patients in the hospital's emergency department from March 1, 2009, to Aug. 31, 2009, whose PHI was on the public website for almost a year.

Stanford acknowledged the breach soon after it was reported publicly but blamed Multi-Specialty Collection Services. Hospital officials claimed they sent the medical information to the collection and billing services firm in an encrypted format but the contractor then created a spreadsheet that was sent to the website for help in creating a graph.

In a statement released after the settlement, Stanford says the Multi-Specialty Collection Services and Corcino & Associates, the owner of the website, will pay $3.3 million of the $4.125 million settlement. The hospital will pay the rest. In addition, the hospital will fund a two-year program that trains medical professionals to protect patient records.

"Patient privacy and data security continues to be an utmost priority at Stanford Hospital & Clinics," the statement said. "We are pleased to have put this case behind us and look forward to helping outside vendors better understand and comply with new patient privacy regulations."

As part of the settlement, each of the affected patients will receive a little more than $100. ✦

HHS releases security risk assessment tool

New tool can assist with HIPAA compliance

A new security risk assessment (SRA) tool to help guide healthcare providers in small- to medium-size offices conduct risk assessments of their organizations is now available from the Department of Health and Human Services (HHS).

The SRA tool is the result of a collaborative effort by the HHS Office of the National Coordinator for Health Information Technology (ONC) and Office for Civil Rights (OCR). The tool is designed to help practices conduct and document a risk assessment in a thorough, organized fashion at their own pace by allowing them to assess the information security risks in their organizations under the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The application, available for downloading at www.HealthIT.gov/security-risk-assessment, also produces a report that can be provided to auditors.

HIPAA requires organizations that handle protected health information to regularly review the administrative, physical, and technical safeguards they have in place to protect the security of the information. By conducting these risk assessments, healthcare providers can uncover potential weaknesses in their security policies, processes, and systems. Risk assessments also help providers address vulnerabilities, which potentially prevents health data breaches or other adverse security events. A vigorous risk assessment process supports improved security of patient health data.

Conducting a security risk assessment is a key requirement of the HIPAA Security Rule and a core requirement for providers seeking payment through the Medicare and Medicaid EHR Incentive Program, commonly known as the Meaningful Use Program.

The SRA tool's website contains a user guide and tutorial video to help providers begin using the tool. Videos on risk analysis and contingency planning are available at the website to provide further context. ✦

Consumer Reports ranks safest hospitals

Consumer Reports has released safety scores for U.S. hospitals by combining five key measures into one composite score from 1 to 100. The score gives consumers a way to compare hospitals on patient safety.

Consumer Reports' hospital Safety Score is comprised of five categories: mortality, readmissions, overuse of CT scans, hospital-acquired infections, and communication. Within the mortality component of the Safety Score, there are two specific measures of hospital mortality:

- medical mortality, in patients who have had a heart attack or been diagnosed with heart failure or pneumonia and who die within 30 days of entering the hospital;
- surgical mortality, for surgery patients who had serious but treatable complications, such as blood clots in the legs or lungs, or cardiac arrest, and died in the hospital.

The data for all of the Safety Score components are the most recent available from the Centers for Medicare & Medicaid Services (CMS). Mortality, readmission, and scanning apply to patients 65 or older; communication applies to all adults; and hospital-acquired infections applies to all ages. Data for hospital-acquired infections is reported by hospitals to the Centers for Disease Control and Prevention (CDC), then to the public through CMS's Medicare.gov website (Hospital Compare).

Surgical patients in top-rated hospitals are at least 34% less likely to die than similar patients in low-rated hospitals.

In medical mortality, only 35 hospitals earned Consumer Reports' top rating, while 66 received the lowest rating. By contrast, more hospitals did well in surgical mortality with 173 earning Consumer Reports' top rating, versus 228 hospitals receiving the lowest rating. However the results are similarly sobering: For every 1,000 surgical patients who develop serious complications in a top-rated hospital, 87 or fewer die. But in a low-rated one, more than 132 die. Surgical patients in top-rated hospitals are at least 34% less likely to die than similar patients in low-rated hospitals.

The article is available in the May issue of *Consumer Reports* and online at http://www.consumerreports.org/cro/magazine/2014/05/index.htm. ✦

HHS final CLIA rule allows reports to patients

In a major change from past policy, the Department of Health and Human Services (HHS) published a final rule amending the Clinical Laboratory Improvement Amendments of 1988 (CLIA) regulations and the Health Insurance Portability and Accountability Act (HIPAA) regulations to permit CLIA-certified laboratories to provide copies of completed test reports to patients (or their representatives) upon request.

The policy change was made possible by including a provision in the CLIA regulations authorizing the release of test results directly to patients and by removing the HIPAA exceptions to an individual's right of access to information maintained by CLIA-exempt laboratories. In the past, HHS has left it up to state law to determine whether laboratories can release test results directly to patients, rather than through their treating providers. Most states prohibit the release of test results directly to patients.

Most states prohibit the release of test results directly to patients.

The preamble to the final rule states that opponents to the move said releasing test results to individuals "without the benefit of provider interpretation and without contextual knowledge that may be necessary to properly read and understand results" could lead to misinformation and unnecessary concern. Many consumer advocates, however, said that increasing access to test results will result in better-informed patients.

Some commenters had suggested restricting access to "sensitive" tests result, such as HIV, cancer, and pregnancy tests. HHS rejected that notion and said patients have a "broad right of access" to health information under the HIPAA Privacy Rule. HHS also said that categorizing testing into "sensitive" and "non-sensitive" categories would be subjective and not necessarily help patients in any way. ✦

CDC wants every hospital to use an antibiotic checklist, improve safety

Reducing prescriptions of high-risk antibiotics in hospitals by 30% could lead to 26% fewer cases of deadly diarrhea infections, according to new advice from the Centers for Disease Control and Prevention (CDC).

A new report from the CDC shows that clinicians in some hospitals prescribe three times as many antibiotics than clinicians in other hospitals, even though patients were receiving care in similar areas of each hospital. In addition, about one-third of the time, prescribing practices to treat urinary tract infections and prescriptions for the critical and common drug vancomycin included a potential error: given without proper testing or evaluation, or given for too long.

... clinicians in some hospitals prescribe three times as many antibiotics than clinicians in other hospitals ...

The report also found that, in hospitals, a 30% reduction in use of the antibiotics that most often cause deadly diarrheal infections with *Clostridium difficile* can reduce these infections by more than 25%. The same antibiotics also prime patients for future super-resistant infections, the report says. The CDC suggests hospitals include these components in an antibiotic reduction program:

- **Leadership commitment:** Dedicate the necessary human, financial, and IT resources.
- **Accountability:** Appoint a single leader responsible for program outcomes. Physicians have proven successful in this role.
- **Drug expertise:** Appoint a single pharmacist leader to support improved prescribing.
- **Act:** Take at least one prescribing improvement action, such as requiring reassessment of prescriptions within 48 hours to check drug choice, dose, and duration.
- **Track:** Monitor prescribing and antibiotic resistance patterns.
- **Report:** Regularly report prescribing and resistance information to clinicians.
- **Educate:** Offer education about antibiotic resistance and improving prescribing practices.

More than half of all hospitalized patients will get an antibiotic at some point during their hospital stay, the CDC reports. The most common types of infections for which hospital clinicians write prescriptions are urinary tract infections, lung infections, and suspected infections caused by drug-resistant *Staphylococcus* bacteria, such as methicillin-resistant *Staphylococcus aureus* (MRSA). The full CDC report is available online at http://tinyurl.com/mn65var. ✦

COMING IN FUTURE MONTHS

- ✦ Why are EMTALA violations rising?
- ✦ *Qui tam* risk higher than ever before
- ✦ Who covers for you on weekends?
- ✦ Cameras in clinical areas: What's allowed?

CNE OBJECTIVES

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

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

CNE INSTRUCTIONS

Nurses participate in this CNE program and earn credit for this activity by following these instructions.

1. Read and study the activity, using the provided references for further research.
2. Scan the QR code below, or log on to **www.cmecity.com** to take a post-test; tests can be taken after each issue or collectively at the end of the semester. First-time users will have to register on the site using the 8-digit subscriber number printed on their mailing label, invoice or renewal notice.
3. Pass the online tests with a score of 100%; you will be allowed to answer the questions as many times as needed to achieve a score of 100%.
4. After successfully completing the last test of the semester, your browser will be automatically directed to the activity evaluation form, which you will submit online.
5. Once the completed evaluation is received, a credit letter will be emailed to you instantly. ✦

CNE QUESTIONS

1. **In the case of Catherine Puetz, MD, suing Spectrum Health regarding her dismissal, what does Philip Becnel, managing partner of Dinolt Becnel & Wells Investigative Group, say was key to making her Facebook post a violation of the Health Insurance Portability and Accountability Act (HIPAA)?**
   A. She named the patient.
   B. She used the patient's initials.
   C. She made a derogatory comment about the patient.
   D. She posted a photo of the patient.

2. **According to R. Stephen Trosty, JD, MHA, CPHRM, president of Risk Management Consulting, what should be considered when judging whether the dismissal of Puetz was justified?**
   A. The federal government is being even stricter when it comes to HIPAA compliance, to enforcement and training by hospitals, and to appropriate action taken for violations.
   B. The federal government recently issued a warning about HIPAA violations on Facebook.
   C. The penalties for HIPAA violations were increased this year.
   D. Any post on Facebook by a healthcare provider and regarding his or her work is a HIPAA violation.

3. **What does Alex J. Brackett, JD, partner with the law firm of McGuireWoods, advise regarding how state laws differ on whistleblower protection?**
   A. Develop a policy unique to each state in which you have a facility.
   B. Develop a systemwide policy that adheres to the most restrictive state laws in which you have a facility.
   C. Develop a systemwide policy that adheres to the least restrictive state laws in which you have a facility.
   D. Do not develop a systemwide policy, but investigate state laws as needed.

4. **According to Clinical Coordinator Dorcas Lewe, RN, MS, at National Children's Hospital, who should notify staff member of a huddle after a patient safety event?**
   A. The CEO or president
   B. The risk manager
   C. The director of human resources
   D. The manager who supervises that person

Legal Review & Commentary

Expert analysis of recent lawsuits and their impact on healthcare risk management

Failure to diagnose premature labor leads to impairments for infant, $42 million verdict

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

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

Angelina Gratiano, Esq.
Los Angeles

News: A mother gave birth to a premature child with multiple physical and cognitive impairments after physicians failed to timely admit the mother to the hospital and subsequently failed to administer treatment that would have prevented brain damage and respiratory distress. The mother alleged that the physicians failed to realize that the woman was in labor at 25 weeks gestation. As a result, the hospital physicians failed to take the necessary steps to protect the child from physical and cognitive impairments. Ultimately, the jury awarded a verdict of $42. 9 million for the parents. The hospital and treating obstetricians were held jointly and severally liable for the child's permanent injuries.

Background: A pregnant woman in her late 20s attended a regularly scheduled prenatal examination at a local hospital for ultrasound examinations and monitoring of her pregnancy. This was not the woman's first pregnancy, and she had experienced a pre-term pregnancy before. During her initial visit with the first evaluating obstetrician, the mother was given a gestational age approximation of 11 weeks. The obstetrician recommended that the woman receive steroid injections, specifically progesterone, starting at week 16 to week 36 of the pregnancy. Additionally, the doctor recommended that the woman's baseline cervix length be measured at week 14 and at week 17 if the cervix length was unusually short.

... the hospital physicians failed to take the necessary steps to protect the child ...

At the next evaluation by the obstetrician, the woman's cervix was growing at a normal rate and was measured at 4.84 cm long. Unfortunately, six weeks later the cervix had decreased to 2.4 cm. Based on the decreasing length of the woman's cervix, the obstetrician recommended a cerclage to sew together the woman's cervix during the remainder of the gestation period to prevent another pre-term pregnancy. A cerclage was performed for the woman shortly thereafter without any problems or complications.

At about four months gestation, the mother returned to the hospital complaining of pelvic pressure. After examination by a doctor, it was discovered that the woman's cervix measured only 1.13 cm in length and additionally physiological changes, namely funneling, were noted. A subsequent ultrasound revealed the presence of excessive accumulation of amniotic fluid within the woman's amniotic sac. These facts were critical in light of the fact that the mother had previously experienced a pre-term pregnancy and delivery at 26 weeks gestation. The excessive amniotic fluid resulted in uterine distention, leaving the woman at a high risk for

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 **Angelina Gratiano**, co-authors, have no relevant relationships to disclose.

premature delivery.

After their examination, the doctors ultimately decided not to provide the woman with any specific instructions regarding bed rest or pelvic rest to ease the pressure in her pelvis. Most notably, however, the doctors also failed to provide steroid treatment for the mother.

On July 2, 2007, in the 25th week of her pregnancy, the woman was admitted to the local hospital and placed on a fetal heart monitor after experiencing frequent severe abdominal pain. However, after three and one-half hours of monitoring, the woman was discharged from the hospital, once again without any special instructions or any course of treatment. Two days later, the woman was admitted to the hospital again after experiencing severe abdominal pain and contractions every 10 minutes. Shortly thereafter, the doctors made the decision to perform an emergency cesarean section.

Although the infant survived the emergency cesarean section, the child was born with many complications. At only 1 pound, 13 ounces, the infant suffered from respiratory distress syndrome, a brain hemorrhage, hearing problems, developmental delay, and gastrointestinal reflux. Over the following two years, the young child required multiple surgeries, various shunt procedures, and insertion of a gastronomy tube (G-tube). To this day, the child requires nutritional care, occupational therapy, physical therapy, and sensory therapy.

The child's mother and father filed suit against the hospital, the obstetrics department of the hospital, the obstetrician responsible for the patient's care, and two other treating physicians. Noting the permanent injuries suffered by the child, the parents alleged joint and several liability against all defendants based on medical negligence. Most notably, the parents alleged that the hospital and treating physicians failed to abide by the required standard of care and course of treatment for a mother who presented pre-term pregnancy symptoms. The jury awarded $42. 9 million in damages after finding the hospital and treating obstetricians liable for medical negligence.

What this means to you: While no case is exactly the same and neither is each patient, it is still extremely important for hospitals to establish protocols for evaluating patient symptoms and diagnoses. In this case, the mother presented with a history of a pre-term pregnancy. Based on this history, the evaluating obstetricians at each point of the woman's second pregnancy should have been on high alert for additional symptoms that could further endanger the woman and her unborn child. This is why organizations such as the American College of Obstetricians and Gynecologists (ACOG) publish standards of care that hospitals and physicians should adhere to.

In this case, the professional standard of care was established by ACOG. It is an established standard of care that a course of steroids is to be administered to a woman who is admitted for early labor or who is at a high-risk pregnancy at 24-34 weeks gestation. It appears that the obstetricians who evaluated the woman were required to ask themselves two questions: one, was the woman in labor and if not, two, is this a high-risk pregnancy at 24-34 weeks gestation? Here, each obstetrician who evaluated the woman after 24 weeks gestation correctly realized that the woman was not in labor. However, the obstetricians failed to consider the next important question in determining how to treat the patient. Consequently, each obstetrician failed to recommend or provide steroid treatment to the woman despite her being within the 24-34 week gestation window during multiple hospital visits.

Had the woman been prescribed steroids by one of the evaluating obstetricians, this prescription would have helped prevent the preterm labor and possibly could have prevented the permanent injuries suffered by the child. By failing to consider both critical questions, the obstetricians and the hospital fell below the established standard of care and were liable for negligence. This case vividly illustrates how crucial it is for medical professionals to be well aware of the required standards of care in light of their individual specialties.

Another important aspect of this case to highlight is the significant damages awarded and what drove the particularly large jury verdict award. Cases involving catastrophic problems to children lend themselves to extremely high damage computations. The cost of future healthcare comprises a large portion of the economic damages in medical malpractice cases. To estimate the total cost of these damages, attorneys must create a life care plan: a detailed evaluation of the anticipated type of care the plaintiff will need in the future, what quality of care the plaintiff will need, how long the care will need to be provided, and what the estimated cost of this care will be.

These life care plans often are prepared by certified life care planners who create the life care plan estimates and then determine the amounts discounted to present value. Extensive documentation and research is required to prepare these plans, including evaluations of alternative options for care and options for future independent living in light of the plaintiff's injuries. In some applicable cases involving children, estimations of how much it would cost to provide education in light of necessary physical accommodations are calculated. Also, the

life care planner typically discounts the plaintiff's award to present value, which is the value of the funds paid to the plaintiff today which, if invested, would generate returns in an amount equivalent to the total future compensation required by the life care plan.

Reference

1. Case No. 002834 (Court of Common Pleas, Philadelphia County, PA) Dec. 20, 2013. ✦

Misdiagnosis of flu instead of pneumonia results in death for 10-year-old girl

News: A 10-year old girl died as a result of complications due to pneumonia after doctors mistakenly diagnosed her with the flu. The child's mother had taken her young daughter to the hospital for symptoms that included fever, vomiting, and respiratory difficulties. Upon evaluation by the late night clinic physician, it was determined that the child was suffering only from a viral flu. She was sent home with her mother without any course of treatment or medication. The following day the woman rushed her ailing daughter to the hospital where the child was pronounced dead as a result of the pneumonia. The parents brought suit against the hospital for medical negligence; however, prior to trial, the hospital made the decision to settle with the family for $265,000.

Background: After complaints of difficulty breathing, fever, and vomiting, a mother took her 10-year-old daughter to a local hospital's after-hours urgent care clinic for evaluation. Due to the time of night, the child was one of the last patients evaluated by the late-night staff before closing. The physician evaluated the girl but only gave her a basic evaluation. Despite noting the young girl's fever, complaints of vomiting, and respiratory distress, the physician dismissed the symptoms as merely a result of a common viral flu. The doctor decided not to order a chest X-ray or even conduct basic diagnostic procedures such as taking the girl's blood pressure readings. The doctor opted not to provide a prescription for a standard course of antibiotics because the doctor was confident the child suffered only from a viral flu.

Pneumonia, while generally treatable, can pose deadly threats if not adequately addressed by physicians. Currently, pneumonia is the eighth leading cause of death in the United States, according to the National Center for Health Statistics. Infants, the elderly, and patients with compromised immune systems are most susceptible to serious cases of pneumonia. If not treated quickly, patients of any age will begin to suffer respiratory failure due to excess fluid in the lungs.

Currently, pneumonia is the eighth leading cause of death in the United States ...

Another important concern that can prove to be fatal is sepsis. Once the infection spreads to the patient's bloodstream, a drastic drop in the patient's blood pressure often leads to cardiac arrest.

Tragically, in this case, the young girl was suffering from a serious case of pneumonia that required immediate treatment. Throughout the night, the mother closely monitored the girl; however, her condition was becoming progressively worse. By the following morning, the woman found her daughter gravely ill. Despite rushing the girl quickly to the hospital, the girl died in the emergency department that morning after succumbing to undiagnosed and untreated pneumonia. An autopsy later confirmed the tragic diagnosis. Sadly, the girl likely was suffering from pneumonia five days prior to her passing.

The parents brought suit against the hospital for negligence for failing to adequately evaluate the young girl despite the seriousness of the symptoms she presented with. Due to the medical caps in California, the family was likely only expecting a maximum of $250,000 for non-economic damages (pain and suffering) based on the Medical Injury Compensation Reform Act. Nine months after the suit was filed against them, the hospital decided to settle with the family for $265,000.

What this means to you: The facts of this case are as simple as they are heartbreaking. The doctor did not adequately evaluate the young girl when she presented with serious symptoms that required additional inquiry and immediate medical attention. As is all too often the case, neglect by medical facilities to establish and/or implement protocols incorporating differ-

ential diagnosis techniques resulted in tragedy. In this case, instead of ensuring that each and every patient received a thorough examination, the doctor provided the child with only a cursory medical exam and neglected serious red flags along the way. It should not matter if the child was the last patient to be admitted to the urgent care clinic that evening. It was the hospital's responsibility to ensure that their physicians provide, to each and every patient, care meeting the required standard.

Another consideration for hospitals is the need to ascertain the right course of action. Often, medical protocols and standards take time to be established, and they might be burdensome or costly to implement. Nonetheless, hospitals should be forward-thinking, and they should aspire toward a higher standard of care than what might be the simple bare minimum. Lawsuits often require the medical community to evaluate the mistakes and pitfalls of other hospitals and physicians because their actions fell below the current required standard of care. Instead, medical professionals should strive to provide the best standard of care possible given the current medical knowledge and treatments. At the very least, however, hospitals must ensure that the established standard of care is met for each and every patient who walks through the hospital's doors.

This case also raises the issue of caps on medical malpractice damages. California law, like other states that implement medical caps for the recovery of damages, severely limits recovery for medical malpractice as further detailed below. That limit creates a serious obstacle for clients and their families who seek compensation for the severity of damages suffered. However, these medical caps can be advantageous to medical facilities as the cap limits the amount the hospital is required to compensate for damages, even though these medical caps are often small in comparison to the lifelong funds frequently needed to adequately care for plaintiffs' permanent injuries.

The history of medical caps in California dates back to 1975 with the enactment of the Medical Injury Compensation Reform Act of 1975 (MICRA). As originally intended, the legislation was supposed to ease the "crisis" created by rising insurance premiums. By setting a limit for amount of recovery of medical malpractice damages, California legislators hoped to encourage physicians to remain in California and to postpone early retirement. Fast-forward almost 40 years later. Some argue the unintended effect of this legislation has been that plaintiffs are less likely to bring medical malpractice lawsuits because of the minimal recovery amount. Since 1975, other states have adopted similar legislation including Indiana, Kansas, Louisiana, Mississippi, Nevada, Oklahoma, West Virginia, and Wisconsin. It should be emphasized that the current California legislation does not place a cap on the amount of money plaintiff's may receive to compensate their medical care, including past and future care. Lost wages or loss of the plaintiff's ability to hold gainful employment as a result of the medical malpractice also are completely recoverable and are not part of the cap amount.

Opponents of the medical caps in California argue that MICRA is preventing juries from awarding a meaningful recovery for the plaintiffs. As it now stands, MICRA limits the amount of recovery for damages, specifically pain and suffering, loss of quality of life, at $250,000. MICRA does not limit the amount a plaintiff is able to recover for medical bills and economic losses, however. Because the cap did not include provisions allowing the limit to be adjusted based on inflation, the current value of $250,000 is only $58,000 in 1975 dollars. If the legislation had included a provision to index the cap based on inflation, the cap would have increased to $1. 1 million, which is the adjusted cap California lawmakers will need to consider. Additionally, trial attorneys also argue that the current cap on damages makes it financially impossible to take on these cases, which often are prolonged and require expensive experts to prosecute correctly. Thus, there is a movement in California to advance a ballot measure that would not only increase the amount plaintiffs may receive for pain and suffering, but also require for doctors to do each of the following:

- use a drug tracking database before prescribing controlled substances;
- undergo random drug and alcohol testing;
- undergo mandatory drug and alcohol testing after a death or injury occurs that was unexpected;
- be required to report any medical negligence or substance misuse they observe by other physicians;
- be put on a mandatory automatic suspension if they test positive for drugs or alcohol.
- report any positive drug or alcohol test results to the California Medical Board.

Physicians from all jurisdictions should closely monitor developments in California as a potential harbinger of similar developments nationwide.

Reference

Case No. KC064431 (Los Angeles County Superior Court, Los Angeles County, CA). Feb. 25, 2014. ✦

HIPAA Regulatory Alert
Cutting-edge information on privacy regulations

Going too far with HIPAA compliance threatens care provided to patients

Overzealous individuals can become the 'HIPAA police'

Healthcare providers have spent years grappling with how to comply with the Health Insurance Portability and Accountability Act (HIPAA), with most of the focus on training clinicians and staff about the dangers of too freely providing protected health information (PHI). Now a new worry is emerging as some providers take HIPAA compliance too far and threaten patient care.

A recent report from the Bipartisan Policy Center, a think tank in Washington, DC, raised the alarm that HIPAA is too far-reaching and "often misunderstood, misapplied and over-applied in ways that may inhibit information sharing unnecessarily." *(See the story on p. 3 for more on that report.)*

The problem can occur in many healthcare settings, but the IT department is a common source. Some hospital IT departments see themselves as "the HIPAA police" and clamp down in ways that HIPAA doesn't require, says **Abraham Gutman**, CEO of AG Mednet, a Boston-based company that assists providers with communication of clinical trial data. Gutman specializes in the de-identification of patient information specific to clinical trials, and he says that with everyone acting as a judge of what HIPAA requires, clinical research and patient care are impeded.

IT departments should publish guidelines on proper HIPAA interpretation to encourage collaboration instead limiting it out of fear, he suggests. The guidelines should explain what is possible in moving data, rather than only focusing on what is prohibited. Explain clearly what safeguards, such as encryption or de-identification, are necessary so that IT managers are willing to try to say "yes" instead of automatically saying "no."

"In my experience the IT departments are among the least knowledgeable about how to comply with HIPAA, but what they do understand is that a breach traced back to them would have very severe consequences," Gutman explains. "Consequently they take the most conservative approach. Nothing can get out, and nothing can get in."

The IT department, however, is sometimes seen by others as authoritative on HIPAA because it is in charge of data transfer. In that case, the IT department's overreaction is passed on to other departments and individuals, eventually creating a culture in the organization that is not based on an accurate HIPAA interpretation but nonetheless hinders data sharing, Gutman explains. *(See the story on p. 3 for an explanation of how the IT department might capitalize on confusion over HIPAA compliance.)*

"It hinders through fear. There is so much fear among the doctor and nurse population that people don't even ask if they can move some data," Gutman says. "They assume from past experience that the exchange will never be approved, so they might as well not ask."

Educate rather than scaring employees

Risk managers, compliance officers, and other administrators should consider whether they are merely scaring employees about HIPAA violations or educating them about the true spirit of the law, suggests **Stephen Cobb**, senior security researcher with ESET, a company based in San Diego that provides IT security for healthcare providers. HIPAA was never intended to prohibit valid data exchanges, but years of scare tactics have made employees fearful, he says.

"What we have ended up with, unfortunately, is a system of compliance that is diametrically opposed to the idea of providing healthcare," Cobb says. "There are some threats to healthcare data, but most of the information threats are for general information rather than people seeking out healthcare data in particular," he says.

Cobb says he is sympathetic with healthcare IT professionals who may be too strict, because they tend to be on the leading edge of understanding what threats exist and how to resist them. Limiting access to data is always key, so he advises working closely with IT staff to develop reasonable policies. "You have to find a way to rein them in if they are going too far, but without diminishing their enthusiasm for security," Cobb says.

Institutions can be guilty of writing HIPAA policies that are overly strict, but more often the problem lies with individuals who do not know the policies or are overzealous in their interpretation, Gutman says. In particular, employees should be reminded that the patient

EXECUTIVE SUMMARY

Healthcare providers can go overboard with efforts to comply with HIPAA, hindering the necessary transfer of patient information. Refusing to provide needed information can threaten patient safety.

- Excessive caution with HIPAA can happen institution-wide or just with individuals.
- The IT department often can be overly cautious with compliance.
- Providers should ensure that staff understand that erring too much on the side of caution can have negative effects.

owns the PHI, not the hospital, he says. Clinical trial participants, for example, explicitly allow the sharing of their information for the purposes of the research, yet some healthcare staff still worry that HIPAA might trump that permission, Gutman says. It doesn't.

"It is important to explain what kinds of data exchanges can be made, with no worries about HIPAA, in all cases as long as these certain criteria are met," Gutman says. "And they must be empowered to act affirmatively in those situations instead of asking someone else's opinion. Once you ask someone else, you're likely to have people say 'no' just to cover themselves."

Individuals fear criminal, civil penalties

Over interpretation of HIPAA became more common in 2013, when HIPAA was amended in an Omnibus Rule that was intended, in large part, to increase certain protections to individuals and for individuals to have greater access to their information, explains **Lani M. Dornfeld**, JD, an attorney with the law firm of Brach Eichler in Roseland, NJ.

The changes also included stiffer penalties for HIPAA violations, including increased money penalties, which triggered covered healthcare providers to amend their HIPAA policies and procedures and re-train staff, she says.

"Although this re-enforced the healthcare industry's obligation to protect patient privacy, it also engendered fear in individual healthcare providers and their staff," Dornfeld says. "They fear both the monetary penalty provisions as well as the criminal penalty provisions of the law. The result is that providers sometimes overshoot. They err on the side of what they believe to be greater protection to the individual who is the subject of the protected health information."

That response sometimes leads to blocking information from others who have a legal right to access such information and whose access would be beneficial to the individual/patient, such as clinicians and administrators.

Staff often misinterpret HIPAA's provisions regarding the amount of information that may be provided to family members and friends involved in a patient's care or in payment for care, as well as what information may be provided to family and friends after a patient's death, Dornfeld says. *(See the story below for more information on difficult situations.)*

Publicity about HIPAA violations encourage fear and overreaction, says **Patricia Wagner**, JD, an attorney with the law firm of Epstein Becker Green in Washington, DC. That reaction is especially prevalent if well-meaning hospital administrators make a point of bringing the incident to staff's attention and reminding them about the need to comply with HIPAA.

"Every incident in the news about HIPAA ratchets up the angst a little more, and people become more cautious," she says.

SOURCES

- **Stephen Cobb**, Senior Security Researcher, ESET, San Diego. Telephone: (619) 203-8317. Email: Stephen.cobb@eset.com.
- **Lani M. Dornfeld**, JD, Brach Eichler, Roseland, NJ. Telephone: (973) 403-3136. Email: ldornfeld@bracheichler.com.

Abraham Gutman, CEO, AG Mednet, Boston. Telephone: (855) 246-3363.

- **Patricia Wagner**, JD, Epstein Becker Green, Washington, DC. Telephone: (202) 861-4182. Email: pwagner@ebglaw.com. ■

Policies should address difficult HIPAA scenarios

There can be murky situations in which the right interpretation of HIPAA is not obvious, says **Patricia Wagner**, JD, an attorney with the law firm of Epstein Becker Green in Washington, DC.

Many of them occur in provider-to-provider transfers, but others can involve family members. For example, a parent or guardian is allowed access to a child's protected health information (PHI) except in certain circumstances. An adult child might seek information about a parent, and interpreting HIPAA might require some investigation into the legal status of the patient or asking the parent to provide permission. "Families can be very complex, and it's not always OK to provide information to everyone in the family," Wagner says.

In addition, there can be confusion among staff regarding state privacy laws that might be more restrictive than HIPAA, Wagner notes. Some organizations also have longstanding habits on data sharing, such as requiring patients to sign consent for sharing information with another doctor, that might not be HIPAA-related, yet HIPAA is cited as the reason for refusal.

Clear policies and procedures can help alleviate some of those problems, Wagner suggests. Without an explicit instruction stating what is and is not required for the data exchange, staff are likely to default to the safest choice of not allowing the transfer, she says.

"The policy shouldn't just reiterate the provisions of the HIPAA rule. It should delineate the exact steps that must be taken to approve the information release,"

Wagner says. "If you get a subpoena, here are the four steps you need to take. Or if you get a request from a parent of a minor, here are the three steps to take and the criteria to check off." ■

Tactical approach takes advantage of confusion

With providers increasingly skittish about violating HIPAA but uncertain about exactly what is required, some IT professionals see an opportunity to improve data security, says **Mick Coady**, principal and co-leader of the Health Information Privacy and Security Practice at PricewaterhouseCoopers, the financial services and consulting company in St. Louis.

This "tactical approach" means IT staff, when asked for help on data exchanges, might overstate what HIPAA requires in order to improve overall data security, Coady explains. They might say that encryption or a certain level of encryption is required for the data, when HIPAA does not require that precaution, for instance.

"Some of the security guys see this as an opportunity to get the tools or policies that they think are necessary in the institution," Coady says. "What they are seeking may be a completely valid need for the provider, but intertwining HIPAA requirements with other security needs in this manner only exacerbates the confusion and encourages more data restriction than HIPAA requires."

SOURCE

• **Mick Coady**, Principal and Co-leader, Health Information Privacy and Security Practice, PricewaterhouseCoopers, St. Louis, MO. Telephone: (314) 565-1949. Email: mick.coady@us.pwc.com. ■

Report finds HIPAA hindering data usage

Overly strict compliance with HIPAA threatens patient safety and quality of care, according to a report from the Bipartisan Policy Center in Washington, DC.

When the think tank released the report, **Esther Dyson**, chairwoman of the group's Health Initiative Coordinating Council, endorsed the findings. "The problem with HIPAA is [that] it was applied much too broadly, and to be candid, it was often used as an excuse not to move data around," Dyson said.

Concerns about privacy and security are sometimes cited as barriers to further progress on the use and exchange of data, the report notes. While HIPAA is designed to safeguard patient privacy, it is often misunderstood, misapplied, and over-applied in ways that might inhibit information sharing unnecessarily, it says. "Additionally, a great deal of data about individuals falls outside the purview of HIPAA, such as consumer-generated data that might be posted on social networks, stored in apps, or shared through other online sources," the authors wrote. "HIPAA specifies how data should be de-identified, but there is considerable variability in the practice of anonymization and no existing standards to govern it. Additionally, some data, such as genomic data, is difficult to adequately anonymize."

Seeking consent from patients to use their data for clinical trials or observational research can help mitigate concerns about privacy, but there is evidence that using "opt-in" or "opt-out" patient data results in bias, the report says. "Robust security also plays a role in building trust," the report adds. "The use of multilayered approaches, combined with other safeguards — such as encryption, tokenization, and access controls — can play a critical role in addressing privacy and security risks, enabling sharing of data, and supporting research that requires more than fully de-identified data."

The full report is available online at http://tinyurl.com/ld54qmp. ■

HHS considering change for background checks

A proposed change to HIPAA might help healthcare providers alert law enforcement agencies that a person's mental illness should be considered when allowing a gun purchase, an action that is made difficult and sometimes impossible by the convergence of HIPAA and state laws.

The Department of Health and Human Services (HHS) recently issued a notice of proposed rulemaking to modify HIPAA. The proposal is to expressly permit certain HIPAA-covered entities to disclose to the National Instant Criminal Background Check System (NICS) the identities of individuals who are subject to a federal "mental health prohibitor" that disqualifies them from shipping, transporting, possessing, or receiving a firearm. *(The proposal is available online at http://tinyurl.com/kg3ad8m.)* The NICS is a national system maintained by the FBI to conduct background checks on persons who might be disqualified from receiving firearms based on federally prohibited categories or state law.

Among the persons subject to the federal mental health prohibitor are individuals who:

• have been involuntarily committed to a mental institution;

• have been found incompetent to stand trial or not guilty by reason of insanity;

• or otherwise have been determined by a court, board, commission, or other lawful authority to be a danger to themselves or others or to lack the mental

capacity to contract or manage their own affairs, as a result of marked subnormal intelligence or mental illness, incompetency, condition, or disease.

Under this proposal, only covered entities with lawful authority to make adjudication or commitment decisions that make individuals subject to the federal mental health prohibitor, or that serve as repositories of information for NICS reporting purposes, would be permitted to disclose the information needed for these purposes.

HIPAA does not specifically prohibit releasing mental health information to the NICS, but it defaults to state laws that might be more restrictive, explains **Lee Lasris**, JD, a healthcare law attorney with the Florida Health Law Center in Davie. The amendment is intended to make clear that HIPAA affirmatively permits — rather than simply not prohibiting — disclosure to the NICS, but Lasris says that might not be enough.

More restrictive state law that prohibits the disclosure still will trump HIPAA unless Congress passes a law saying otherwise, Lasris says.

"The amendment will have an impact only in states that do not have more restrictive laws. They will have a clear statement from HHS that HIPAA does not prevent this reporting, and that may be helpful," Lasris says. "In states with more restrictive laws, their solution will be to work with the state legislatures to effect those changes."

SOURCE

• **Lee Lasris**, JD, Florida Health Law Center, Davie Telephone: (954) 358-0155. Email: llasris@flhealthlaw.com. ■

Health system uncovers inside data breach

Riverside Health System in Newport News, VA, has fired an employee and is offering free credit monitoring to several hundred patients affected by a privacy breach that involved records covering four years.

The breach was discovered during a random company audit, according to a statement by company spokesperson **Peter Glagola**. After an investigation, Riverside's Compliance Department determined that an employee had inappropriately accessed 919 medical records spanning September 2009 through October 2013. The information accessed included patients' social security numbers, a summary of the patient history, and other information that appears in Riverside's electronic medical record.

The employee was fired, and Riverside is contacting the patients affected by the breach. All will be offered complementary three-bureau credit monitoring. The company has attempted to send notification letters to all patients and next of kin to those known to be deceased, but it has been unable to locate current contact information for all affected patients. ■

HHS to survey 1,200 — Audits might follow

The Department of Health and Human Services' (HHS') Office for Civil Rights (OCR) announced that it will survey up to 1,200 covered entities and business associates to find those in need of a full HIPAA compliance audit.

The survey will collect information such as the "number of patient visits or insured lives, use of electronic information, revenue, and business locations." The Health Information Technology for Economic and Clinical Health (HITECH) Act requires OCR to conduct periodic audits to ensure that covered entities and business associates are complying with the HITECH Act and its implementing regulations.

An audit of 115 covered entities in 2012 found that compliance issues with the HIPAA Security Rule. About two-thirds of audited entities did not have a complete and accurate risk assessment, and many entities were unaware of specific HIPAA Privacy Rule requirements, such as the obligation to provide a notice of privacy practices to individuals. ■

First ever settlement with local government

In the first settlement with a local government, the Department of Health and Human Services (HHS) reached an agreement with Skagit County, WA, about HIPAA violations.

The dearartment previously reached a settlement with the state Medicaid agency in Alaska, but it has never reached a settlement with a local breanch of government.

The county's troubles began on Dec. 9, 2011, when Skagit County reported to HHS that it had inadvertently provided public access to the protected information of seven individuals. HHS then discovered that the breach was larger. Skagit County had inadvertently uploaded files containing the protected health information (PHI) of 1,581 individuals onto a public web server.

The HHS Office for Civil Rights (OCR) investigated the county's privacy and security practices and found what it calls "widespread non-compliance" with the HIPAA privacy, security, and breach notification rules. The investigation ended recently with a resolution agreement that requires Skagit County to pay $215,000 and adhere to a stringent remediation and reporting program. ■

Healthcare Risk Management

2014 Reader Survey

In an effort to learn more about the professionals who read *HRM*, we are conducting this reader survey. The results will be used to enhance the content and format of *HRM*.

Instructions: Fill in the appropriate answers. Please write in answers to the open-ended questions in the space provided. Return the questionnaire in the enclosed postage-paid envelope by **July 1, 2014.**

1. Please fill in all the areas for which you are responsible for risk management in your facility or system.

- O A. acute care
- O B. outpatient services
- O C. same-day surgery
- O D. home health services
- O E. rehabilitation services
- O F. extended care facility
- O G. hospice

In future issues of *HRM*, would you like to see more less coverage of the following topics?

	A. more coverage	B. less coverage	C. about the same amount
2. compliance	O A	O B	O C
3. malpractice	O A	O B	O C
4. patient safety	O A	O B	O C
5. patient restraints	O A	O B	O C
6. informed consent	O A	O B	O C
7. patient confidentiality/privacy	O A	O B	O C
8. patient falls	O A	O B	O C
9. medical errors	O A	O B	O C
10. root-cause analysis	O A	O B	O C
11. sentinel event reporting	O A	O B	O C
12. accreditation issues/audits	O A	O B	O C

13. Do you find the *Legal Review & Commentary* insert in *HRM* helpful?

O A. yes O B. no

14. Including *HRM*, which publication or information source do you find most useful, and why?

_____

_____

15. Do you plan to renew your subscription to *HRM*?

- O A. yes
- O B. no If no, why not?_____

_____

16. Are the articles in *HRM* written about issues of importance and concern to you?

- O A. always
- O B. most of the time
- O C. some of the time
- O D. rarely
- O E. never

17. How would you describe your satisfaction with your subscription to *Healthcare Risk Management* newsletter?

- O A. very satisfied
- O B. somewhat satisfied
- O C. somewhat dissatisfied
- O D. very dissatisfied

18. Which best describes your title?

- O A. risk manager or risk management director
- O B. VP or assistant administrator
- O C. director/manager of quality
- O D. medical director or director of nursing
- O E. other_____

19. Please indicate all of the activities for which you have primary management responsibility.

- O A. risk management
- O B. compliance
- O C. legal
- O D. quality or utilization review
- O E. other_____

20. Which area at your facility triggered the most incident reports in 2013?

- O A. emergency department
- O B. medical
- O C. obstetrics
- O D. operating room
- O E. other _____

Please rate your level of satisfaction with the following items.
A. excellent B. good C. fair D. poor

21. Quality of newsletter	○ A	○ B	○ C	○ D
22. Article selections	○ A	○ B	○ C	○ D
23. Timeliness	○ A	○ B	○ C	○ D
24. Length of newsletter	○ A	○ B	○ C	○ D
25. Overall value	○ A	○ B	○ C	○ D
26. Customer service	○ A	○ B	○ C	○ D

27. On average, how many people read your copy of *HRM*?

○ A. 1
○ B. 2
○ C. 3
○ D. 4
○ E. 5 or more

28. What is the bed size of your facility/system?

○ A. fewer than 200 beds
○ B. 200 to 400 beds
○ C. 401 to 600 beds
○ D. 601 to 800 beds
○ E. more than 800 beds

29. On average, how many articles in *HRM* do you find useful?

○ A. none
○ B. 1-2
○ C. 3-4
○ D. 5-6
○ E. 7 or more

30. What do you like most about *HRM* newsletter?

31. What do you like least about *HRM* newsletter?

32. Please list the top three challenges you face in your job today.

33. What issues would you like to see addressed in *HRM* newsletter?

Contact information