35th Anniversary

Healthcare RISK MANAGEMENT

February 2014 | Vol. 36, No. 2 Pages 13-24

GWU's victory shows value in fighting fraud charges

Qui tam *case dragged on for 16 years, but hospital comes out on top*

With hospitals defending themselves from all manner of civil cases and federal prosecution, a big win for a provider is reason to celebrate. The recent victory for George Washington University (GWU) Hospital in Washington, DC, is welcome news, even if it took 16 years.

Employees of the hospital alleged that it billed for services of anesthesiologists when the doctors did not perform all aspects of the anesthesia care. The allegations led to a *qui tam* case in which the federal government joined to claim that the hospital had defrauded the government of Medicare funds because of improper coding for the anesthesia services. *(See the story on p. 15 for more on the details of the case.)*

GWU was represented by William D. Nussbaum, JD, and Jonathan L. Diesenhaus, JD, of the law firm Hogan Lovells in Washington, DC. They declined to comment on the victory and GWU also refused, except to say they were pleased with the outcome.

The judge's ruling in the case suggests that the years of haggling eliminated so much evidence that the case just fell apart, says **Nicholas D. Jurkowitz**, JD, a healthcare attorney with the law firm of Fenton Nelson in Los Angeles, who represents hospitals. Whatever evidence was left after both parties argued over admissibility was insufficient to sustain the case, he says.

> *"... individuals face significant obstacles when suing such a large institution."*

The outcome suggests that, despite the False Claims Act and *qui tam*, individuals face significant obstacles when suing such a large institution, Jurkowitz says.

"The institution is a much bigger entity and has far more resources for fighting, but in addition, all of the information is within the institution," he says. "The hospital has all the information. For the individuals, even if they have seen something and have some knowledge, it is harder for them to access this information and move forward."

The outcome of the case should be

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.

heartening to risk managers who fear that individuals can make claims against a hospital and then have the federal government jump on board with a bias toward finding fraud, says **Mark Kadzielski**, JD, an attorney with the law firm of Pepper Hamilton in Los Angeles.

"This is a decision that we have seen in other cases where allegations have been made but were not proven under the False Claims Act, and plaintiffs were procedurally given the chance to put up or shut up," he says. "If they can't, then the case is thrown out. This is reassuring in a sense that you can't take a large institution to court with allegations like this and expect there to be some assumption of fraud or some largesse in terms of a settlement."

Executive Summary

George Washington University (GWU) Hospital in Washington, DC, has prevailed in an 16-year-old lawsuit accusing the hospital of False Claims Act violations. Legal analysts say the outcome should be encouraging to health-care risk managers.

- ✦ The case involved allegations of anesthesia billing fraud.
- ✦ Plaintiffs might have been hampered by the extensive nature of the allegations.
- ✦ Risk managers should assess the reporting mechanisms available to staff members who suspect fraud.

What impacted the case?

Plaintiffs in the GWU case were hampered in part by their own expansive allegations of fraud, which required gathering records from numerous physicians and patients that went back to 1989, before the current GWU management and before current methods of document storage, Kadzielski notes. *(Some legal analysts predict more fraud claims in the future. See the story on p. 15 for more information.)*

Eighteen years is an extremely long time for such a case to drag out, and Jurkowitz points out that even the victory must have cost GWU a fortune in legal expenses. Even with in-house counsel, such litigation usually is handled by outside attorneys, he notes.

The GWU case is a reminder to assess your own compliance programs, Jurkowitz says. In particular, he suggests assessing whether there is a mechanism in place, a person who can be contacted easily and without fear of repercussion, when a low-level employee suspects fraud. "Sometimes people at the bottom of the totem pole are reluctant to speak up, especially if there is no easy way for them to report it without putting themselves in jeopardy," he says. "Their fears might be overcome if they realize they can file suit and potentially reap a big reward."

Fighting early might be best

The case is a reminder that the hospital must take an aggressive stance with fraud charges from the beginning, says **Mark H.M. Sosnowsky**, JD, an attorney with the law firm of Drinker Biddle & Reath in Washington, DC. Don't focus

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.)

so much on the potential liability that you are moved to settle or admit wrongdoing before making the plaintiffs prove their claims, he says.

Case law has given the government some advantages when litigating false claims, but hospitals still can demand that the plaintiff prove individual allegations, Sosnowsky notes. Often, the hospital's best opportunity comes in the motion-to-dismiss stage, when it can aggressively demand proof and have some allegations thrown out. After that, the fight gets more difficult and more expensive.

"You have to make the relator demonstrate their case early on, and in this case the hospital did file motions for dismissal and whittled down the allegations to the point that it won on summary judgment," Sosnowsky says. "These cases are imminently winnable, but you do have to have the stomach for this kind of fight and the potential for significant damages. That is what makes litigating a case like this extremely risky."

SOURCES

- **Nicholas D. Jurkowitz**, JD, Associate, Fenton Nelson, Los Angeles. Telephone: (310) 444-5244. Email: njurkowitz@fentonnelson.com.
- **Mark Kadzielski**, JD, Attorney, Pepper Hamilton, Los Angeles. Telephone: (213) 928-9820. Email: kadzielskim@pepperlaw.com.
- **Mark H.M. Sosnowsky**, JD, Associate, Drinker Biddle & Reath, Washington, DC. Telephone: (202) 354-1327. Email: Mark.Sosnowsky@dbr.com. ✦

Hospital whittled down claims to reach summary judgment

A federal judge recently determined that there is no admissible evidence left to accuse George Washington University (GWU) of overbilling the government for anesthesia services, which ended a marathon legal fight that began in 1998.

That was the year that four certified registered nurse anesthetists (CRNAs) formerly employed by GWU filed a lawsuit claiming that the hospital submitted false claims to Medicare for reimbursement of anesthesia procedures. The claims were fraudulent, they alleged, because GWU regularly said the anesthesia procedures had been performed entirely by a licensed anesthesiologist when parts of the anesthesia process had been performed by residents or CRNAs.

The hospital and the plaintiffs fought for 16 years, with GWU able to systematically eliminate many of the claims. Finally U.S. District Judge **Colleen Kollar-Kotelly**, JD, issued an 18-page opinion that ended the saga by granting GWU's motion for summary judgment. "As the factual background tracing the slow narrowing of this case shows, relators have not provided any evidence that would be admissible at trial to prove their allegations as to 2,579 medical procedures for which they assert GWU knowingly submitted a false claim," she wrote. The court had upheld objections by GWU in the past year that precluded plaintiffs from introducing evidence related to 2,162 of the total 2,579 Medicare claims.

Two newer orders held that the remaining alleged false claims also were unsupported by admissible evidence.

"As a result of these rulings, and the rulings coming before them, there is no longer a 'genuine dispute as to any material fact' regarding whether GWU knowingly submitted false Medicare claims," the judge wrote. "In short, in light of the various motions *in limine* limiting the evidence on which relators can rely, relators lack a triable case in this matter. The court has no choice but to grant summary judgment on the body of evidence (or lack thereof) before it." ✦

False claims, antitrust risks on the rise

Even with the recent victory by George Washington University (GWU) in its long-running false claims case, hospitals should not rest easy, cautions **Keith Lavigne**, senior vice president of ACE USA Professional Risk, an insurance and reinsurance company based in Philadelphia, PA. False claims and antitrust cases are on the rise, he says.

The False Claims Act is the government's primary tool for combating waste, fraud, and abuse by healthcare providers participating in federal healthcare programs and by other government contractors, Lavigne notes. Billions of dollars have been collected under the False Claims Act via a multitude of actions brought directly and indirectly by the Office of Inspector General, Department of Justice, whistleblowers, and billing auditors.

According to the Department of Justice, in the last three decades, recoveries have increased from a couple of hundred million dollars per year to almost $6 billion for 2013, with the proportion of recoveries from medical service providers increasing from less than 10% to more than 60%. To support the Office of Inspector General and the Department of Justice in their pursuit to crack down on fraud and abuse, other recent anti-fraud enforcement initiatives include the creation of special Health Care Fraud Prevention and Enforcement Action and Medicare Fraud Strike Force teams.

Perhaps the most aggressive of all the new initiatives was Congress' authorization for the Department of Health and Human Services, through

its Centers for Medicare and Medicaid Services division, to implement programs run by third-party contractors whose primary purpose was to identify, correct and collect improper overpayments, Lavigne says. "With compensation for some of these auditors directly tied to recoveries, hospitals can expect to continue seeing an increase in medical record requests from these third-party auditors," he says.

Healthcare providers also face increased risk that their activities will run afoul of the federal antitrust laws, he cautions. Over the past four years, federal and state enforcement agencies, along with the private bar, have significantly ramped up their efforts to police anticompetitive conduct. While price-fixing, agreements to allocate markets, and monopolization remain staples of antitrust litigation, we have entered a new age of antitrust liability for healthcare providers. Investigations, challenges, and lawsuits have targeted numerous types of conduct. Anything that unreasonably restrains competition can pose antitrust risk in most industries, including healthcare, he explains.

"... hospitals can expect to continue seeing an increase in medical record requests from these third-party auditors."

"The growing edge for antitrust appears to relate to mergers and acquisitions. Consolidation — born of early healthcare reform and spurred by the Affordable Care Act — is being checked by a swelling tide of enforcement actions and private lawsuits," Lavigne says. "Hospital acquisitions of physician practices, mergers among physician practices, and providers consolidating with other types of providers all carry antitrust risk if they lead to the exercise of market power in the form of higher prices or reduced quality of care or access."

Healthcare market participants should not expect an abatement of vigorous antitrust enforcement, Lavigne says. The market forces that are driving the tidal wave of consolidation and the struggle for shifting and shrinking reimbursement dollars will be present for the foreseeable future.

"Because healthcare providers face more scrutiny than ever before, it is important that risk managers, in-house counsel, and compliance teams work together to develop a proactive enterprise risk management strategy to mitigate these exposures," he says.

SOURCE

• Keith Lavigne, Senior Vice President, ACE USA Professional Risk, Philadelphia, PA. Telephone: (215) 640-1000. Email: keith.lavigne@acegroup.com. ✦

Risk managers merging employee health with patient safety

Risk managers have become finely attuned to the health and safety of patients, but what about the doctors, nurses, and other medical staff who care for them? More often than not, the safety of healthcare workers is overlooked because patients are the primary focus, some experts say.

As a result, more than 2 million reported lost work days due to on-the-job injuries are sustained annually by workers in the healthcare industry, says **Scott Harris**, PhD, MSPH, director of EHS Advisory Services for Underwriters Laboratories Workplace Health and Safety, a consulting group based in Franklin, TN. He says risk managers are beginning to pay more attention to the financial ramifications and bottom-line impact of neglecting the safety and health of hospital and other healthcare employees.

"The numbers are huge. If I told you you had a $79,000 water leak, you'd probably go in there and fix that."

Harris studies the effects of worker injuries in the healthcare industry and says the costs are growing. For injuries sustained in 2011, the costs to healthcare employers totaled about $13 billion, but that number climbed to $13.9 billion for 2012. The worker population also went up in that timeframe, and the rate of injuries remained about the same.

"There seems to be a gentle shift toward a more serious injury," Harris says. "The leading type of injury by far is overexertion back injuries, which is double or triple anything else. That typically is associated with patient handling, tripping, and falling, often all at the same time."

The average injury cost also is rising, currently at about $79,000 per injury. When the cost of injuries is spread over the entire healthcare workforce, the cost comes to about

$870 per worker, he says.

"You can look at that as a tax or a fee or whatever, but if you look at your entire workforce, you can expect to spend almost $900 a head for lost-time injuries this year," Harris says. "The numbers are huge. If I told you you had a $79,000 water leak, you'd probably go in there and fix that."

Hospitals account for half of the costs and close to half of the injuries, even though they don't employ half of the healthcare work force, Harris notes. *(For information on how the Occupational Safety and Health Administration might become more involved with healthcare injuries, see the story on p. 18.)*

Work with your cohorts

Employee health also is a growing concern for **Grena Porto**, RN, MS, ARM, CPHRM, healthcare practice leader with ESIS Health, Safety and Environmental in Philadelphia and former president of the American Society for Healthcare Risk Management (ASHRM) in Chicago. Employee health and patient safety always have been closely intertwined, she says, but there also has been an effort to delineate the responsibility for the two.

"We've had employee health and risk management, and for a long time they were completely separate departments that just happened to have a lot of the same concerns," Porto says. "We were both concerned about falls and the cost of injuries that happened on the premises, but we in risk management always focused more on the patient."

Executive Summary

Some hospitals are putting more focus on the cost of employee injuries. Risk managers are ideally suited to assist because of their expertise with patient safety.

✦ The average employee injury will cost a hospital $79,000.

✦ Hospitals can expect to pay about $900 per employee each year for injury costs.

✦ Most hospital injuries are related to overexertion of the back, slips, and falls.

Acknowledging the overlap does not necessarily mean that two departments should be merged or that the employee health duties should be heaped onto the already overflowing plate of the risk manager. Rather, risk managers should look for ways to work cooperatively with their counterparts in employee health and avoid duplicating efforts, she says.

Harris suggests that risk managers might play a role in investigating and preventing worker injuries because their field has concentrated so effectively on patient safety in recent years, whereas employee health professionals can get bogged down in the financial management of injuries after they happen. Risk managers also might have some expertise in exploring the true costs of an injury that are sometime not so obvious.

"A lot of times when we talk with employee health professionals, they will be able to cite the insurance costs and the time off work as expenses, but we normally see that their estimate of the cost of those 20 injuries last year was lower than it actually was," Harris says. "We try to focus on the real numbers, how that nurse being out for two weeks with a knee injury is going to cost you on average $79,000."

Hospital administrators typically do not treat patient injuries and worker injuries the same, Harris notes. They put much more emphasis on injuries occurring to patients, he says. *(See the story below for more on the perceived difference.)* That disparity is partly because patients are the focus in healthcare, and nurses often are tough people who are accustomed to working injured, he says.

"But at the end of the day safety is safety, and you can't say one group is more important than another when it comes to safety," Harris says. "The effort the healthcare industry has put into patient safety is admirable and there's no call to back away from it, but that only shows what could be done with the same effort in employee safety."

SOURCES

• **Scott Harris**, PhD, MSPH, Director of EHS Advisory Services, Underwriters Laboratories, Franklin, TN. Telephone: (615) 312-1320.

• **Grena Porto**, RN, MS, ARM, CPHRM, Healthcare Practice Leader, ESIS Health, Safety and Environmental, Philadelphia. Telephone: (610) 220-8500. Email: grena.porto@esis.com. ✦

Do you treat worker injuries like patient injuries?

When trying to explain why hospitals should pay as much attention to worker injuries as to patient injuries, **Scott Harris**, PhD, MSPH, director of EHS Advisory Services for Underwriters Laboratories Workplace Health and Safety, a consulting group based in Franklin, TN, has a favorite question to ask hospital administrators.

He starts by asking if it is a big deal in their facilities for a patient to

fall on the floor. Unanimously the administrators roll their eyes and exclaim about all the investigations that must follow, the paperwork to be completed, reports to be made, and the prevention efforts to undertake. Oh yes, they say, it's a big deal.

But what happens when a nurse falls?

"The room gets quiet and they say, well, it's not really the same, that's a different situation," Harris says. "But it's really the same thing. No one should be hitting the floor. Even from a purely financial and legal perspective, even if you take out the human side of caring for your employees' well-being, it should be a very big deal to you when a nurse falls, just the same as when a patient falls." ✦

OSHA might take a closer look at healthcare injuries

The federal agency that oversees workplace injuries may soon look more closely at the healthcare industry, says **Scott Harris**, PhD, MSPH, director of EHS Advisory Services for Underwriters Laboratories Workplace Health and Safety, a consulting group based in Franklin, TN.

Among other changes, the Occupational Safety and Health Administration (OSHA) soon might require quarterly filing of the OSHA 300 logs on employee injuries, which would make that information public, Harris notes. That filing would be a change from the current situation in which hospitals must log the data, but it rarely becomes public unless OSHA expresses a particular interest. The proposal is in a comment period.

"Interestingly, OSHA said one of the reasons for making that data public would be for employees to decide if that was someplace they wanted to work. So you could have someone interviewing for a job and saying they're not sure because your back injury rate is twice the national average," Harris says. "And they said customers could decide if the safety of that location means they want to do business there."

> *"... customers could decide if the safety of that location means they want to do business there."*

Harris has heard other indications that OSHA is ready to increase scrutiny of hospitals and other providers. Even bringing the level of attention up to normal would be a dramatic change, Harris says. The healthcare industry is inspected less than most employers with comparable injury rates, Harris says, and the OSHA fines tend to be less than in other industries — typically half or two-thirds of what other industries might experience.

"That probably has been part of the problem. We all know that OSHA can come and inspect your hospital, but it's just not likely, and people in the industry know that," he says. "Unfortunately the fear of OSHA and the money they can take from you is a big motivator for action in any industry, and healthcare has gotten off easy in that regard for some time now." ✦

Your 'nicest' patient could sue you for malpractice

It is a fact of life that the squeaky wheel gets the grease, but that should not be true when it comes to patient safety. Risk management experts caution that the most compliant, seemingly satisfied patient can be the one who ends up suing for malpractice if that easygoing demeanor leads staff to lower their standards.

Patient safety can be threatened when a patient is compliant and does not complain, notes **R. Stephen Trosty**, JD, MHA, CPHRM, president of Risk Management Consulting in Haslett, MI, and a past president of the American Society for Healthcare Risk Management (ASHRM) in

Executive Summary

The patient who is most compliant and never complains could inadvertently lead staff to provide substandard care. If the patient is harmed, it will be no defense to say that the patient reported satisfaction with the care provided.

✦ Caution staff to watch for the natural tendency to direct more care to the most vocal patients.

✦ Ensure that the standard of care is maintained for all patients, regardless of their personalities.

✦ Encourage staff to speak up when a patient appears to be neglected.

Chicago. Trosty cautions risk managers to educate staff about the risks posed by an easygoing patient, especially if the staff is pushed to the breaking point. When there are not enough hands to go around, it might be the "nice" patient who is neglected, he says, but the fact that the patient seemed satisfied will be no defense in a malpractice case.

Consider the hypothetical case, prompted by actual incidents, of an elderly man admitted to a hospital for routine surgery. On the first day of recovery, family members complain that he is being neglected by staff. Surprisingly, multiple staff members divulge that the hospital is short-staffed on weekends and therefore unable to provide all the expected care.

Physical therapy is not provided twice a day as scheduled, the patient is not encouraged to use the spirometer, he is not offered aid to get to the bathroom, and he is left sitting in a chair all day because he told staff he was "fine" and did not complain about being left there. At one point, staff fail to respond to calls for walking assistance for 45 minutes, and when help finally comes, the patient has soiled himself. Despite all this, he tells family members that "the staff were just as nice as could be."

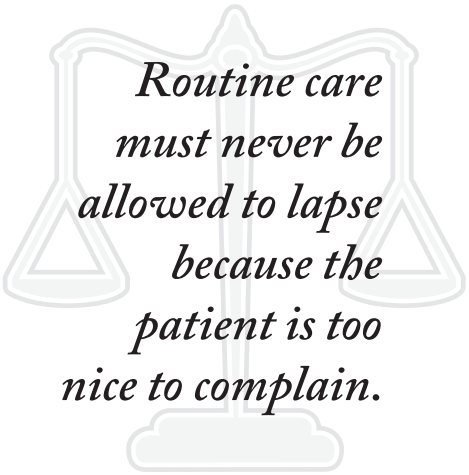
The family understands that the man's personality is such that he is unlikely to complain about his care, and he also has little understanding of what constitutes neglect. If the patient suffers any adverse event or poor outcome, the family and plaintiffs' attorneys will understand that his care was substandard whether he wants to complain or not.

And if a malpractice lawsuit results, the hospital would be ill-advised to defend itself by saying the patient was satisfied, Trosty notes.

Overcome natural tendency

The problem is not the patient, of course, but the natural human tendency to respond most to those asking for assistance or complaining about the quality of care. Though understandable, that tendency must be overcome with professionalism, scheduling and adequate staffing, Trosty says.

"It should not make any difference what type of patient you have in terms of receiving care. Care should be provided on set schedules, based upon patient needs and regular rounds of staff," he says. "The answering of call buttons should have nothing to do with the cooperativeness of patients. If it does make a difference, then a problem with staff has been identified. If staff do let it matter, then they have to be violating existing policies or at least policies that should be in place regarding responding to the needs of all patients."



That approach will work until staff members are overwhelmed by multiple patient needs occurring at the same time, Trosty notes, and then it is probable that the cooperative patient might not receive the first response. Attention might instead be directed to the patient or whose family is the greatest complainer.

That situation should exist only in extreme circumstances and rarely, if at all, Trosty says. Routine care must never be allowed to lapse because the patient is too nice to complain. If it does, Trosty says, the hospital is critically understaffed or the staff is unprofessional — or both.

Staff members should be reminded that their "dream patient" could be the one who ends up injured and suing the hospital if they let their guard down, says **Jane McCaffrey**, DFASHRM, MHSA, director of compliance and risk management at The Blood Connection in Greenville, SC, and a past president of ASHRM. "There are protocols that need following, and missed therapies need immediate evaluation," McCaffrey says. "Any facility that has staff providing quality care based on who complains the loudest has bigger problems, and I doubt any patient got what was needed."

McCaffrey takes the notion a step further and wonders about the negative impact of patient satisfaction initiatives such as not turning on a light at night to check on a patient or turning down alarms or overriding them. Those strategies might be designed to improve patient satisfaction scores, but McCaffrey wonders if they threaten patient safety by encouraging staff members not to bother the patients who seem content.

She is not the only one to wonder about how much to let sleeping patients lie. **John C. Metcalfe**, JD, FASHRM, vice president of risk management services with MemorialCare Health System in Fountain Valley, CA, recalls hearing of a related issue from the risk manager of another California facility. In that hospital, a patient care attendant elected not to turn on a bedside light to fix a lead on a female patient. The patient was extremely startled and thought that the attendant was doing touching her inappropriately. She was upset even after the charge nurse told her that the man was fixing the lead at his direction.

Not turning on the light and ensuring that the patient was awake prior to touching her became an allegation of abuse investigation and reportable event. As a result, Metcalfe says the nursing educator for acute care services at the facility in question now conducts educational role playing for this scenario.

SOURCES

• **Jane McCaffrey**, DFASHRM, MHSA, Director of Compliance and Risk Management, The Blood Connection, Greenville, SC. Telephone: (864) 751-3092. Email: jjmccaffrey49@gmail.com.

• **John C. Metcalfe**, JD, FASHRM, Vice President, Risk Management Services, MemorialCare Health System, Fountain Valley, CA. Telephone: (562) 933-2000. E-mail: jmetcalfe@memorialcare.org.

• **R. Stephen Trosty**, JD, MHA, CPHRM, President, Risk Management Consulting, Haslett, MI. Telephone: (517) 339-4972. E-mail: strosty@comcast.net. ✦

Tail insurance is an increasing concern as industry changes

As hospitals take on more physicians and buy more group practices in response to the move toward accountable care, risk managers are dealing more and more with the question of tail insurance.

Covering the physician's past activities always has been an option if the hospital wanted to woo a particularly desirable physician group, but now the volume of acquisitions is forcing a harder look at the value of tail insurance — and the inherent risks. Aside from the cost considerations, offering tail insurance can lead to violations of federal regulations, cautions **Linda M. Robison**, JD, a partner with the law firm of Shutts & Bowen in Fort Lauderdale, FL.

"It's a real regulatory nightmare. Hospitals have to be extremely careful if you offer tail insurance, even the ones that are captive," Robison says. "They have to make doggone sure that the cost of that tail coverage, when considered with the physicians' salary, won't bust the stock problem."

The tail is a liability of the group, Robison explains, and therefore the group is responsible for buying tail coverage. Sometimes a hospital wants to acquire a physician group so much that it will require the group to purchase the tail insurance but promise to increase compensation enough to make up for the cost.

Or in some cases it is not necessary to offer compensation. Robison says she routinely advises hospital clients to require that physicians buy their own tail coverage as part of the contract terms, with no mention of the hospital paying for it in any way.

Assisting the physician practice with paying for tail insurance is not necessarily a bad idea, but Robison says there is a serious risk that the deal will violate regulations requiring fair market value for the physician group.

> *... there is a serious risk that the deal will violate regulations requiring fair market value for the physician group.*

"It could be viewed as a purchase for the referrals, even though the doctors are going to be employees," Robison explains. "I would never allow a hospital client to risk a Stark violation for paying top dollar to a doctor and then buying some really expensive tail coverage. The claim will be that the tail exposure was never a liability of the hospital's and so they only paid it to get those referrals."

Look at value of the insurance

The value of the insurance is a major determinant of whether the deal is too sweet, Robison says. In some states where doctors often go bare or have only minimal coverage, the malpractice coverage for physicians probably is not very expensive and so the tail market coverage is not, either. In those cases, a hospital might be able to include tail coverage without pushing the overall value of the acquisition past fair market value, Robison explains. The balance becomes more difficult to achieve as the cost of the insurance rises.

The evaluation must include all the factors that make up the total purchase price of the practice, such as relocation expenses and the purchase of assets. If other purchase factors are on the high end of the scale, that will leave you less room to maneuver with the cost of tail insurance before you break the bank, Robison says.

Another complicating factor is

Executive Summary

Hospitals are offering tail insurance as part of their efforts to recruit physicians and physician groups, but the move comes with potential risks. Not only can the coverage be expensive, but it also can lead to regulatory violations.

✦ Offering to pay for tail insurance could make the overall purchase price too high.

✦ Paying more than market value for a practice can be a Stark violation.

✦ The risk manager might have to veto offers that are too lucrative.

the physician's specialty. Tail coverage for neurosurgery, orthopedics, or obstetrics, for example, will be much more expensive than some other specialties because the potential for lawsuits and large awards is much greater.

The hospital also must evaluate the tail coverage policy to look for hidden risks and issues that affect the value of the insurance. The coverage period for the tail is the first question, of course. Does the policy cover any demand for care provided in the tail period up to the statute of limitations, or is there a more limited period when the policy will apply?

"You have to look at the total package of what you're paying for this acquisition and be comfortable that it is still within the fair market value," Robison explains. "Put all the numbers on the table and figure out how close you are to a violation. It might be the risk manager's job to put the brakes on and say, 'Whoa, there's a limit to what we can offer here, no matter how much we want this practice.'"

SOURCE

• Linda M. Robison, JD, Partner, Shutts & Bowen, Fort Lauderdale, FL. Telephone: (954) 847-3850. Email: lrobison@shutts.com. ✦

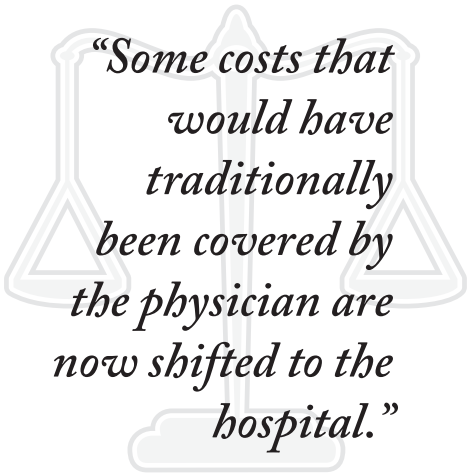
Med-mal cost growing at slowest rate in 14 years

The cost of medical malpractice is growing at the slowest rate in the 14-year history of the Aon/ASHRM Hospital and Physician Professional Liability Benchmark report. The 2013 report was released recently by Aon Risk Solutions, the global risk management business of Aon, with the American Society of Healthcare Risk Management (ASHRM).

"We project zero growth in the number of malpractice claims," says **Erik Johnson,** healthcare practice leader for Aon's Actuarial and Analytics Practice and author of the analysis. "Healthcare professional liability claims are subject to a complicated set of geographic, societal, and technological influences. These forces are largely in-check, resulting in a low inflationary environment for medical malpractice."

New in this year's report is the use of hospital admissions and revenue as a basis for benchmarking medical malpractice cost levels. The report estimates that in 2014 medical malpractice claims will represent $0.60 per every $100 of hospital revenue or an average of $135 per hospital admission.

Healthcare organizations are achieving efficiencies and savings by employing physicians and using their self-insurance facilities to cover medical malpractice, Johnson says. The cost savings are achieved by promoting patient safety, creating uniformity of risk management, and jointly defending claims, when they happen. However, Johnson warns, "some costs that would have traditionally been covered by the physician are now shifted to the hospital."



Risk management involvement and investment in patient safety have translated into improved medical malpractice results, says **Ron Calhoun**, managing director of Aon Risk Solutions Healthcare practice. "Hospitals are focused on containment of traditional risks such as medical malpractice while they take on new opportunities introduced by the Affordable Care Act and the transition from fee-for-service models and into outcome-based models," he says.

These are additional findings in the report:

• Projected loss rate for hospital professional liability is $2,940 per occupied bed equivalent (OBE) for events occurring in 2014. The frequency of claims is projected to be 1.67% per OBE, and the severity of claims is expected to be $176,000 per claim.

• Projected loss rate for physician professional liability is $6,030 per physician for events occurring in 2014. The frequency of claims is projected to be 2.97% per physician and severity of claims is expected to be $203,000 per claim.

• Projected loss rate for hospital general liability is $119 per occupied bed equivalent. The average general liability claim is expected to be $36,000 for claims occurring in 2014.

• Projected loss rate for obstetrics claims occurring in 2014 is $171 per birth; for the emergency department, the projected loss rate is $6.16 per visit.

• The hospital professional liability benchmark database includes claims from all U.S. states and provides specific benchmarks for 28 states. Florida ($7,440) and

Pennsylvania ($4,720) have the highest projected loss rates for 2014. Indiana ($800) and Minnesota ($810) have the lowest projected loss rates for 2014.

To purchase a copy of the *2013 Hospital Professional Liability and Physician Liability Benchmark Analysis*, go to http://tinyurl.com/llvsxql. The cost is $269 for ASHRM members and $369 for others. ✦

Long-term care liability costs on the rise

Liability costs for long-term care providers are expected to increase by 5%, and claims frequency also is expected to rise, according to an analysis released recently by the American Health Care Association (AHCA) and Aon Global Risk Consulting, the risk consulting business of Aon. The report also indicated that plaintiff firms have focused attention on states with more vulnerable legal climates.

Across the country, long-term care and post-acute care centers provide care for 1.1 million frail and elderly and employ more than 1.5 million people, notes **Mark Parkinson**, president & CEO of AHCA. Rising liability costs drive up the cost of doing business and not only threaten access to care, but ultimately could cost jobs, he says.

The "2013 Long Term Care General Liability and Professional Liability Actuarial Analysis" provides estimates of loss rates, or the cost of liability to the beds that care providers operate. The projected national 2014 loss rate, which is a combination of claim severity and frequency, is $1,940 per occupied bed. This number means that an operator with 100 beds can expect $194,000 in liability expenses in 2014.

Kentucky's loss rate, the highest of the profiled states in the study, has been increasing since 2008 and is projected to reach $8,090 in 2014. Kentucky's state constitution prohibits limits on tort recoveries, and there are no statutes concerning qualification of expert witnesses, certificates of merit, pre-trial alternative dispute resolution, or limits on attorney's fees. West Virginia, the state with the second highest loss rate among the report's profiled states, has a reputation for high verdicts and a challenging appellate system.

Texas reports the second lowest loss rate in the study: $300 per occupied bed. The state experienced dramatic loss rate reductions following constitutionally protected tort reform in 2003. These reductions in loss rates have been sustained in the years following the legislation.

The study also examined claims resolved through arbitration agreements and discovered that the agreements often lead to resolution in a similar timeframe, but with a lower cost. The average cost of a claim under an arbitration agreement is $155,000, while a non-arbitrated outcome averages $184,000, which makes arbitrated outcomes 16% less costly. ✦

CMS issues rule on Stark exceptions

The Centers for Medicare & Medicaid Services (CMS) has released a final rule that revises the exception to the federal physician self-referral prohibition (known as the Stark Law) for certain arrangements involving the donation of electronic health record (EHR) items and services.

The rule addresses what is known as the Stark Exception. The Office of Inspector General (OIG) of the Department of Health and Human Services simultaneously released a companion rule revising the safe harbor regulation concerning EHR items and services under the Federal Anti-Kickback Statute, known as the Safe Harbor.

CMS and OIG amended the final rules from 2006 as part of an ongoing effort to encourage the adoption of EHR systems. The systems can be too expensive for some physician practices, and hospitals have been interested in assuming some of the costs.

These were the five key changes in the amendment:

- The Stark Law exception and the Safe Harbor are extended until Dec. 31, 2021.
- After March 27, 2014, laboratory companies will no longer be protected donors.
- The EHR software is deemed

interoperable if, on the date the software is provided to a physician, a certifying body authorized by the National Coordinator for Health Information Technology certifies that the software meets the then-applicable EHR certification criteria.

• The rule clarifies the requirement prohibiting any action that limits or restricts the use, compatibility, or interoperability of donated items or services.

• The electronic prescribing capability requirement is removed. ✦

TJC issues NPSG on clinical alarms

The concern over "alarm fatigue" and other threats to patient safety from clinical alarms has led The Joint Commission (TJC) to issue a new National Patient Safety Goal (NPSG) on the topic. The new NPSG requires accredited hospitals and critical access hospitals to improve their clinical alarm systems.

The alarm NPSG is in an educational phase and is focused on improving awareness of the potential risks associated with clinical alarms. The second phase begins Jan. 1, 2016, and introduces requirements to control the patient safety risks posed by the alarms.

The new NPSG was deemed necessary after providers reported deaths attributed to alarm fatigue ...

The new NPSG was deemed necessary after providers reported deaths attributed to alarm fatigue, in which clinicians become overwhelmed by the many alarm signals they hear and purposefully ignore them or just tune them out because of sensory overload. Clinicians can be subject to hundreds of alarm signals every day, the TJC reports, and they sometimes turn down the volume or adjust alarm parameters outside of safe limits. The Joint Commission Sentinel Event database reported eight alarm-related deaths from 2009 to 2012. The Food and Drug Administration database reported 566 deaths between January 2005 and June 2010, according to the TJC report.

In October 2011, TJC and other groups collaborated to find ways to immediately improve clinical alarm safety, and the NPSG is one of the results. *(The new NPSG can be found online at http://tinyurl.com/alarmnpsg. For* Healthcare Risk Management's *previous reporting on alarm fatigue, see the June 2013 issue, p. 68.)* ✦

COMING IN FUTURE MONTHS

✦ Hospital program prevents bedsores

✦ EMTALA compliance: New challenges

✦ Medication event huddles

✦ Who covers for you on weekends?

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. **How did George Washington University (GWU) Hospital prevail in its 16-year case in which former employees alleged false claims?**
   A. A federal judge recently determined that there is no admissible evidence left to accuse GWU of overbilling the government for anesthesia services.
   B. A federal judge recently weighed the evidence and issued a ruling in favor of GWU.
   C. A federal judge recently accepted GWU's argument that the plaintiffs did not have standing to bring the case.
   D. A federal judge recently agreed with GWU that the scope of the document requests by the plaintiffs exceeded what could be reasonable and prudent.

2. **What was the basis for the lawsuit alleging false claims involving GWU?**
   A. Employees of the hospital alleged that it billed for surgery that was not performed and also for surgery that was not necessary.
   B. Employees of the hospital alleged that it billed for services of anesthesiologists when the doctors did not actually perform all aspects of the anesthesia.
   C. A group of physicians claimed that GWU excluded it from participation in services by billing for services at a rate below market value.
   D. A group of physicians claimed that GWU improperly attributed therapy services to them while actually retaining the reimbursement for the hospital.

3. **According to Scott Harris, PhD, MSPH, director of EHS Advisory Services for Underwriters Laboratories Workplace Health and Safety, which of the following is true of worker injuries in healthcare?**
   A. The average injury cost is falling, currently at about $39,000 per injury.
   B. The average injury cost is holding steady, currently at about $59,000 per injury.
   C. The average injury cost is holding steady at about $69,000 per injury.
   D. The average injury cost is rising, currently at about $79,000 per injury.

4. **According to Linda M. Robison, JD, a partner with the law firm of Shutts & Bowen, which of the following is true?**
   A. Tail insurance can be prohibitively expensive, but it poses no regulatory risk.
   B. The Stark Law requires hospitals to provide tail insurance for acquired physician groups.
   C. In most situations, insurers will not provide tail insurance to a hospital wishing to purchase it for an acquired physician group.
   D. Tail insurance can result in a Stark violation if the value causes the overall purchase price to exceed fair market value.

Legal Review & Commentary

A Monthly Supplement to HEALTHCARE RISK MANAGEMENT

Excessive bleeding after childbirth leads to mother's death, over $15 million in damages

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.
Associate Attorney
Law Office of Steven Carvel, Manhattan Beach, CA
Los Angeles

News: A 33-year-old woman died due to excessive bleeding shortly after childbirth when the two physicians overseeing her care failed to follow established protocol for the woman's high-risk pregnancy. The woman's treating obstetrician failed to note the unique location of the woman's placenta, as the woman suffered from a condition known as placenta accreta. This condition left the woman abnormally vulnerable to a high risk of hemorrhaging during childbirth because her placenta was not as easily removable as in other more common pregnancies. While this condition can be readily diagnosed with well-established imaging techniques and protocols, the physicians overseeing the woman's care failed to request imaging to ensure her placenta had developed properly. Tragically, when the physicians realized the abnormal location of the woman's placenta, it was too late. One of the obstetricians made the decision to separate the woman's placenta from the uterus during the cesarean section, but the physician did not request that additional emergency care, such as extra blood and platelets for blood transfusion and additional nursing and surgical staff, be made immediately available. Without additional blood and staff on hand, the woman's condition rapidly deteriorated, and the woman eventually bled to death. After a two-week trial, the jury deliberated less than six hours before finding both doctors in charge of the woman's care, along with the hospital where the woman was treated, jointly and severally liable for medical malpractice, and imposed $15. 55 million in damages.

... when the physicians realized the abnormal location of the woman's placenta, it was too late.

Background: A 33-year-old woman received prenatal care during her pregnancy by her treating obstetrician. During a woman's pregnancy, regular visits with her obstetrician are critical to ensure that the pregnancy is progressing normally. At this point, between 15-20 weeks of gestation, the woman's obstetrician requested an obstetrical ultrasound. A separate obstetrician, a specialist in prenatal imaging, failed to properly interpret the woman's ultrasound and failed to diagnose the condition placenta accreta.

While not a concern for most women, placenta accreta is a condition in which the woman's placenta develops with an abnormal attachment to the myometrium. Essentially, the placenta develops through the endometrium, rendering the removal of the placenta during

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 relationships to disclose.

childbirth particularly dangerous. Because the placenta for a woman suffering from placenta accreta has developed with abnormal depth, its removal from the uterine wall causes severe hemorrhaging.

In this case, the woman's condition was not diagnosed before childbirth, which is not entirely uncommon. Placenta accreta can be difficult to diagnose before birth. However, established imaging techniques and protocols can aid obstetricians in establishing a diagnosis. If this condition is suspected, the treating obstetrician might be able to take proactive steps to ensure the safety of the mother and the baby during childbirth.

Three major medical organizations have established physician guidelines for placenta imaging, including the American College of Radiology, the American Congress of Obstetricians and Gynecologists, and the American Institute of Ultrasound in Medicine. All three organizations emphasize the need for physicians to obtain images that show the relationship between the woman's cervix and the placenta during pregnancy. To ensure the physician understands the relationship between the structures, both structures should be included in the same image. In this mother's case, the obstetricians failed to ensure that these images were done in accordance with the established guidelines, such that the physicians did not determine the relationship between her cervix and her placenta. This mistake was a critical one, as the failure to do their due diligence in understanding the relationship between these structures ultimately led to incorrect interpretations of subsequent imaging done on the woman.

Additionally, the obstetrician overseeing the woman at the hospital during her delivery failed to request an ultrasound prior to conducting the woman's cesarean section. An ultrasound image should be done prior to a cesarean section to ensure the placenta is not abnormally attached to the woman's cervix. In this case, by failing to conduct an ultrasound of the woman prior to her surgery, physicians were not aware how deeply attached the woman's placenta was to her cervix. By the time the physicians began the cesarean section and removal of her placenta, they realized that the placenta was so deeply embedded in the cervix that they could not prevent the excessive bleeding.

Lastly, the physicians treating the woman failed to request additional resources prior to the woman's cesarean section. In this case, the doctors failed to request additional blood for a transfusion as well as additional nursing and medical staff to handle any complications. The failure to have additional blood on hand led to the woman bleeding extremely quickly without sufficient blood on hand with which to transfuse her. Unfortunately, the woman died due to excessive bleeding. However, her child was born and survived the cesarean section.

The woman's husband filed a wrongful death suit against the two treating obstetricians and the hospital overseeing her cesarean section, and he asserted joint and several liability. After a two-week trial, the jury found both doctors and the hospital guilty of medical malpractice based on joint and several liability. The jury gave the verdict and awarded the husband $15.55 million in damages after deliberating less than six hours.

What this means to you: When there are established guidelines from professional medical organizations, physicians should heed these guidelines because these guidelines create the professional standard of care expected by reasonable professionals in the doctor's field. Most importantly, it is best not to take shortcuts on these guidelines to ensure proper due diligence has been performed. In this case, had the obstetricians followed the guidelines set out by medical organizations regarding ultrasounds during pregnancies, the doctors would have understood how deeply embedded the woman's placenta was and that removal of her placenta would result in serious medical complications. Instead, the physicians relied on the interpretation of a single ultrasound read by an individual radiologist. They did not view that ultrasound or order additional ultrasounds toward the end of the pregnancy or at the time of the c-section. Relying on one individuals' interpretation of critical information can be problematic. Had they considered the risk factors of a previous c-section and advanced maternal age, they might have made a more thorough assessment of the placental relationship with the uterus.

Another consideration for physicians is the assurance that the hospitals they practice in are prepared for emergencies in the different high-risk specialty areas such as the emergency department, surgery, and labor and delivery. There should be emergency codes that can be called by staff when things go awry, such as a "Code OB Hemorrhage" or a "Code OB. " These rapid response codes ensure needed emergency equipment, blood, drugs, and staff members are given to the patient in minutes. Admitting patients to and practicing in hospitals without these life-saving processes in place can lead to very unfavorable outcomes for both parties.

Additionally, it is important for physicians to actively participate in the current and developing medical knowledge in their respective fields. Keeping up to date with emerging medical knowledge helps ensure that doctors and hospitals are well aware of important issues in the medical field. This step can be accomplished by proactively engaging in attending conferences, seminars, subscribing to medical journals, and even by attend-

ing networking dinners or events. Research yields new developments and viewpoints concerning even well-known complications and diseases. Medical professionals who presume that they are above carving out time for continuing professional education run a significant risk of steering themselves and their patients into an adverse outcome that could have been avoided by keeping up with the cutting edge of the profession.

Ultimately, doctors and hospitals want to ensure that they provide the best medical care possible. To do so, due diligence must be done to ensure that the doctors and the hospital are prepared to handle patient needs.

Reference

Case No. 09-L-012356 (Cook County Circuit Court, Cook County, IL). Nov. 22, 2013. ✦

Delayed bacterial infection diagnosis leads to $9.5 million verdict

News: New parents noticed their 2-week-old child had missed some feedings and was not behaving normally. The parents then decided to bring the child to the emergency department of a nearby hospital. When the results from the blood test came back positive for Group B streptococcus (GBS), the child's parents were not informed immediately and neither was the child's pediatrician. The emergency department staff waited two days to inform the parents and the treating pediatrician that the child tested positive for GBS. Unfortunately, at this point, the infection spread quickly throughout the infant's system, reached her brain, and caused meningitis. By the time the parents eventually were told to bring the child back to the local hospital to admit the child, the child already had developed cerebral palsy, a permanently debilitating condition. The hospital settled the case. After an 11-day jury trial, the jury found the emergency nurse and the emergency department medical group liable for professional medical malpractice and awarded $9. 5 million in damages.

Background: The young child's parents brought the child to the emergency department of a nearby hospital after observing the child's decreased appetite and abnormal breathing patterns. The parents patiently waited six hours in the emergency department to find out what was wrong with their child. However, after a blood sample was drawn for further testing, the parents were told to return home with the child as it was very likely that the child was suffering only from a cold. Within hours, the blood results indicated that a bacterium was present in the vulnerable child's system. The hospital laboratory immediately called down to the hospital emergency department to relay the results: The gram stain tested positive for GBS. An emergency nurse was told the results, but tragically this information was not immediately provided to the emergency physician who evaluated the child.

Additionally, the emergency nurse failed to contact the parents or the child's pediatrician to inform them that bacteria was present in the child's bloodstream and ask that the child be brought back to the hospital for emergency medical treatment. When the emergency physician finally became aware of the blood culture results two days later, indicating that the GBS bacteria was present in the infant's blood, he advised the parents to bring the child back to the hospital to be admitted immediately.

GBS generally is carried in the intestines and lower genital tract. While normally not a serious problem for adults with well-developed immune systems, GBS does pose a significant danger to newborns. If GBS is carried by pregnant women, it becomes a danger to the infant during delivery. Most hospitals test women for GBS during prenatal care or during the early stages of labor. If present, antibiotic therapy is given to the mother, and the child is protected from developing the infection.

Unfortunately, by the time the parents were informed, the infection had developed into meningitis, and it caused seizures in the child's brain. The emergency physician and nurse delayed informing the parents about the lab results. By doing so, precious time was wasted, as the child urgently needed medical attention.

When the first test came back indicating that bacteria was in the child's blood, GBS should have been considered, and the child's parents should have been instructed to bring the child back to the emergency department immediately. Two days after initially bringing the child to the emergency department, the parents were informed that GBS can result in meningitis and that the problem needed to be addressed quickly now. By this point, it was too late, as the child already had suffered irreparable damage to her young body and brain. As instructed by the emergency physician, the parents brought the child to the hospital to be admitted. But after treatment long overdue, the parents were informed the child had developed cerebral palsy at the young age of less than three weeks old.

The parents subsequently brought

suit against the hospital, the emergency department medical group, and the nurse overseeing the child's care in the emergency department. Prior to trial, there was a confidential settlement agreement with the hospital, but the case proceeded against the emergency department medical group and the emergency nurse. Ultimately, the emergency department medical group and the emergency nurse were held jointly and severally liable for the child's irreparable damages after an 11-day trial. The jury awarded the $9. 5 million in damages, which included $5 million for future medical bills and expenses, $1. 5 million awarded for lost earnings, and $3 million for non-economic damages, such as pain and suffering. However, pursuant to the law in the applicable state, non-economic damages are subject to a cap of $650,000.

What this means to you: While it is often difficult to keep track of timelines during emergency medical care, it is important that well established protocols be kept and maintained to ensure that patients and treating physicians are informed as soon as possible regarding time sensitive test results. Various hospitals have different systems in place for ensuring that results are provided to the right contact immediately; for example, time logs. In this case, the nurse responsible for contacting the parents and pediatrician about the test results allowed too much time to go by before informing someone. It is unfortunately not uncommon for test results to be overlooked once a patient leaves a busy emergency department. If the results are not directly recorded electronically into the emergency department chart, it is even more difficult to manage. They often are found later in either a miscellaneous file in the emergency department that no one has responsibility for, or returned to the medical record department to be filed in the emergency department chart at a later date. As electronic recordkeeping advances and improves, most systems are able to capture test results in the medical record as soon as available. But that does not negate the responsibility for someone to gather the results of ordered tests and bring them to the attention of the treating physician for follow-up orders. Medical staff rules and regulations typically require that the treating physician review the results of all tests ordered, even if the patient has been discharged. A nurse might be assigned the duty of bringing these results to the physician for review; however, it should not be the nurse's responsibility to decide if a test result is normal or abnormal. Unless the nurse has advanced practice credentials, such as a nurse practitioner or physician's assistant, the responsibility falls to the physician. However, once the physician determines that a test result is abnormal, he or she can delegate notification of the patient to the nurse. The physician should electronically sign that the results have been reviewed, and the nurse should document that the results were called in to the patient with additional instructions given if required.

Some electronic medical records come with an indicator, such as a red flag, that a new result has been received. The indicator remains until the result is signed off as being seen by the physician. These types of electronic alert systems work well to ensure that nothing is missed. Whatever system is in place to notify physicians and patients of test results, it needs to be monitored and tested periodically for accuracy and effectiveness. This point assumes added importance as electronic recordkeeping becomes increasingly common throughout all pivot points in the healthcare delivery system.

It is important to note that the nurse in charge of relaying the time sensitive lab results to the parents and pediatrician testified that she recalled "having concerns" about the infant and it had generally been her normal practice as a nurse to inform doctors of any problems or delays in a patient's treatment. An infant at two weeks of age is a prime target for becoming septic with GBS. The mother should have been questioned about being tested for GBS during her pregnancy. Given the danger of becoming ill very quickly, the child should have remained in the emergency department to receive emergent medical care until it was ruled out. This case is thus a strong example of how vital it is to stick to one's instincts as a medical professional. The nurse knew that the child was in danger of suffering severe and permanent damage based on the type of bacterial infection, so it is likely that the nurse knew in her professional experience that keeping a good track of the test results was exceptionally important to this child's treatment. Clinicians should use their medical experience, knowledge, and general practices to make sure that they follow the necessary procedures involved in medical care. They should have back-up systems in place for times when the electronic data is down. And they should follow through on the medical plan for the patient. If you are ordering a test, there must be a reason. That reason does not disappear when the patient leaves the office or facility. Clinicians need to understand how and when physicians are to be notified of pending test results and when and how any abnormal results will be communicated to the patient. While the nurse was culpable because of her oversight, the physician has the ultimate responsibility to complete the circle of care.

Reference

Case No. CAL 11-08836 (Prince George County Circuit Court, Prince George County, MD), Nov. 22, 2013. ✦

HIPAA Regulatory Alert

Supplement to *Healthcare Risk Management* and *Hospital Access Management*

HIPAA enforcement is increasing, and industry experts expect scrutiny in 2014

Role and obligations of business associates still in question

Healthcare providers are under the gun more than ever when it comes to compliance with the Health Insurance Portability and Accountability Act (HIPAA) because of recent changes that make it easier for the government to learn of breaches and to prosecute them, warns **Stephen Treglia**, JD, legal counsel at Absolute Software, a consulting firm in Austin, TX, that assists healthcare providers with HIPAA compliance.

A primary change spurring the increased enforcement was the Health Information Technology for Economic and Clinical Health (HITECH) Act. Before HITECH, Treglia explains, HHS had to rely solely on submitted complaints to become aware of HIPAA violations. *(See the story on p. 2 for more on what is driving the increased enforcement.)*

Changes to the definition and responsibilities of business associates (BAs) also are leading to conflicts that could complicate data security and make things messy if one occurs, Treglia says. "There's a big battle between providers and business associates," he says. "Business associates are trying to deny they are associates and making it hard for the covered entities that want them to become HIPAA-compliant. That's never good when two parties that both have a lot to lose can't work together to comply with the regulation."

Even if you're not arguing with your BAs, a covered entity might put too much confidence in the BA agreements (BAAs) required by HIPAA. Simply having one in place does not shield the healthcare provider from liability in the event of a breach, Treglia has learned.

Treglia recently attended a meeting with Leon Rodriguez, the Office for Civil Rights (OCR) director who has since been nominated to become the Director of the United States Citizenship and Immigration Services office of the Department of Homeland Security. Rodriguez told attendees at the meeting that the OCR was hiring more staff and planning to conduct more audits of HIPAA compliance. The subject of BAAs came up, and Treglia asked Rodriquez if having one in place was sufficient to protect the covered entity from liability related to a breach caused by the BA. Many covered entities seem to think so, Treglia told Rodriquez.

"Is it more in the form of governance that you're seeking?" Treglia asked the OCR director.

"That's exactly what we're looking for," Treglia recalls Rodriquez replying. "We're not looking for a one-shot relationship between the business associate and the covered entity. It's more of a partnership in which the covered entity should be providing guidance and governance to their business associates as to how to protect their patients' information."

The struggle to define BAs and refine the working relationship regarding HIPAA will likely continue for a couple of years, Treglia says. Rodriguez told the group including Treglia that OCR is taking "a very broad view of the definition of business associates."

"So that is probably where the battleground is coming up next," Treglia says.

More class action lawsuits

In addition, Treglia says the plaintiffs' bar has seen gold in the hills of HIPAA. Banking on support from a more empowered HHS to prosecute data breaches, trial lawyers are eager to file class-action lawsuits against entities that have been identified as

EXECUTIVE SUMMARY

The Department of Health and Human Services (HHS) is enforcing the Health Insurance Portability and Accountability Act (HIPAA) vigorously, and the push is likely to continue. Data breaches are more likely to be discovered now even if the provider doesn't report them.

- Prior to the Health Information Technology for Economic and Clinical Health (HITECH) Act, HHS relied on complaints to become aware of HIPAA violations.
- Business associates and covered entities continue to disagree over their roles and responsibilities.
- Class action lawsuits involving data breaches are on the rise.

having their medical records breached.

"When HHS prints a public listing of the breached entities, that makes them sitting ducks for class action suits," Treglia says. "A lawyer can go down the list and see who has the deepest pockets."

But what about encryption? Isn't that the solution that everyone proposes for HIPAA compliance? If the data is encrypted, even a stolen laptop full of protected health information (PHI) doesn't amount to much of a problem, according to many experts.

Treglia is more skeptical about encryption being the ultimate solution. He points out that encryption only works when the person attempting to access the data doesn't have the decryption keys, and sometimes they do. HIPAA data breaches have involved healthcare provider employees with access to decryption keys, Treglia notes. Huping Zhou, a former UCLA Healthcare System surgeon, was the first person sent to prison for intentionally viewing the PHI of co-workers, supervisors, and celebrities after being told he was fired, and encryption would not have stopped him, Treglia says.

"We're most aware of the loss of data, when someone steals a laptop for instance," Treglia says. "But we're realizing now that hacking is a real threat as well, in which the data never leaves your facility and there is no indication that a breach has occurred. The data has been compromised, and that's a breach just as much as a laptop left at Starbucks."

Treglia's advice is to expect 2014 to be a tough year for HIPAA compliance.

"We've only seen the tip of the iceberg. This trouble with business associates and the other issues, that is only going to increase in the years ahead," he says. "The enforcement push is not going to slow down in the near future."

SOURCE

• **Stephen Treglia**, JD, Legal Counsel, Absolute Software, Austin, TX. Telephone: (512) 600-7455. ■

HITECH led to current enforcement push

The Health Information Technology for Economic and Clinical Health (HITECH) Act and the subsequent Omnibus Final Rule have dramatically increased the likelihood that unauthorized releases of protected health information (PHI) will be discovered, for several reasons, says **Stephen Treglia**, JD, legal counsel at Absolute Software, a consulting firm in Austin, TX.

Treglia outlines the effects:

• The HITECH Act empowered certain federal and state agencies to pursue investigations. On the federal side, the Office for Civil Rights (OCR) was given the authority to investigate complaints and conduct random audits.

• HITECH also granted jurisdiction to all state attorney generals to pursue Health Insurance Portability and Accountability Act (HIPAA) and HITECH investigations.

• HITECH changed who is responsible for identifying PHI breaches, imposing a breach notification requirement to OCR for any unauthorized release of PHI.

• The Omnibus Final Rule increased the likelihood of enforcement actions for HIPAA-HITECH violations by permitting the Department of Health and Human Services (HHS) to develop regulations providing for the distribution of collected monies for successful investigation to complainants, offering the means to reward whistleblowers for information provided to OCR.

• The Omnibus Final Rule made it easier to enforce HIPAA's Privacy Rule and Security Rule by changing the burden of proof when a breach occurs. Previously, once a breach occurred, the violating entity simply could allege no harm resulted from the breach and it would be up to the complainant to prove harm existed. The Omnibus Final Rule has reversed that situation. Now, once a breach occurs, it is up to the violating entity to disprove harm occurred. ■

Compliance program must be strong

Case resulted in $150,000 settlement

What might seem like a rather minor data breach could lead to bigger problems if it opens the door to investigators taking a look at your entire Health Insurance Portability and Accountability Act (HIPAA) compliance program. That situation is what happened with Adult & Pediatric Dermatology (APDerm) of Concord, MA, which recently settled allegations of HIPAA violations for $150,000.

APDerm will be required to implement a corrective action plan (CAP) to correct deficiencies in its HIPAA compliance program. APDerm is a private practice that delivers dermatology services in four locations in Massachusetts and two in New Hampshire. This case marks the first settlement with a covered entity for not having policies and procedures in place to address the breach notification provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA), notes **Shannon Hartsfield Salimone**, JD, a partner with the law firm of Holland & Knight

in Tallahassee, FL.

The Office for Civil Rights (OCR) in the Department of Health and Human Services (HHS) opened an investigation of APDerm upon receiving a report that an unencrypted thumb drive containing the electronic protected health information (PHI) of about 2,200 individuals was stolen from a vehicle of one its staff members. The thumb drive was never recovered.

The investigation revealed that APDerm had not conducted an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality of PHI as part of its security management process, according to a statement from the OCR. Further, APDerm did not fully comply with requirements of the Breach Notification Rule to have in place written policies and procedures and train workforce members.

"As we say in healthcare, an ounce of prevention is worth a pound of cure," said OCR Director **Leon Rodriguez** said in announcing the settlement. "That is what a good risk management process is all about: identifying and mitigating the risk before a bad thing happens. Covered entities of all sizes need to give priority to securing electronic protected health information."

HHS found in its investigation that the practice did not conduct an accurate and thorough security risk analysis until more than one year after the breach. Additionally, the covered entity did not implement the requirements of the HIPAA Breach Notification Rule to have written policies and procedures and train its workforce members until Feb. 7, 2012. In the settlement agreement, the practice did not admit liability, but HHS refused to concede that the practice was in compliance.

Among other things, the CAP requires the practice to, within one year, conduct a new risk analysis, and then to develop a risk management plan that must be reviewed and approved by OCR. The practice also must report any HIPAA violations to OCR within 30 days. The full terms of the settlement are available online at http://tinyurl.com/DermSettlement.

Although the $150,000 payment is not extraordinary, Salimone says the case illustrates how healthcare providers can find themselves in quicksand once data is compromised. "From the settlement, it was clear they were not being penalized just for the breach," she says. "Instead, it seems this was the result of what the Office for Civil Rights perceived as a lack of compliance with the basic requirements of the security rule. All covered entities are required to do a documented risk analysis, which presumably would have turned up the fact that this practice wasn't being as careful as it should on training employees."

The case also illustrates how doing the right thing by reporting a data breach can prompt more trouble than the breach itself. "From an enforcement perspective, no good deed goes unpunished. That seems to be the entry point for a lot of these Office for Civil Rights enforcement activities," Salimone says. "To me it seems a little bit unfair to just go after these folks who have done the right thing by reporting, and it would be more fair to have some sort of random auditing. But they don't have the budget for that, and I'm not sure that's on the horizon."

Because any breach could invite investigators in for a close look at your HIPAA compliance program, it is important to evaluate your program for any shortcomings and constantly improve, Salimone says. *(See the story below for the most common failings of a HIPAA compliance program.)*

"If you have a breach and you can show that you had those protections in place ahead of time and you did everything you could reasonably to prevent it, I think you're going to be less subject to penalties," Salimone says.

SOURCE

• **Shannon Hartsfield Salimone**, JD, Partner, Holland & Knight, Tallahassee, FL. Telephone: (850) 425-5642. Email: Shannon.salimone@hklaw.com. ■

EXECUTIVE SUMMARY

A dermatology practice recently settled allegations of privacy law violations for $150,000. The fine and other sanctions appear to be the result of systematic failures in the compliance program rather than the breach itself.

• Even a small breach can open the door to an inspection of your entire program.

• This is the first settlement regarding a failure to have policies and procedures for breach notification.

• The settlement includes a corrective action plan.

7 most common failures in compliance programs

Frequent re-evaluation of your Health Insurance Portability and Accountability Act (HIPAA) compliance plan is a good idea, but what do you look for? Start with the most common shortcomings that the experts see in efforts to comply with HIPAA.

Shannon Hartsfield Salimone, JD, a partner with the law firm of Holland & Knight in Tallahassee, FL, offers this list of the most common problems she encounters with HIPAA compliance plans:

• Writing a notice of privacy practices and stopping there. The notice is not enough. It must be backed up by appropriate policies and procedures.

• Not updating your notice or policies and

procedures. Maybe you wrote a notice of privacy practices in 2003 that was entirely adequate, but have you updated it since then? The Health Information Technology for Economic and Clinical Health (HITECH) Act and the security rule required substantive changes in the notice and the policies and procedures backing it up.

• Failing to adequately train employees. Even the best policies and procedures are worthless if your employees don't understand them and put them into action. "HIPAA is extraordinarily complex and detailed in terms of what it requires of covered entities, and a lot of providers don't have the resources or the desire to devote enough to the training," Salimone says. "Training your people well doesn't guarantee the Office for Civil Rights will go easy on you if you do have a breach, but failing to train will be much likely to lead to a substantial fine."

• Not providing a link on your web site to the notice of privacy practices. This requirement is easily achieved, but it is also easily overlooked. "If that link is not there, it tells me that someone did not go through each of the requirements and make sure they were fulfilled, because that is clearly stated in the rules," Salimone says.

• Failing to do an adequate documented risk analysis. There is no set way to do the analysis, Salimone says, but it often involves the use of outside technicians and consultants to test the firewalls and encryption practices. Many covered entities do no risk analysis or do an inadequate one that is carried out by the same people who designed the protections.

• Skimping on the policies and procedures. If your HIPAA policies and procedures manual is 10 pages long, Salimone says you might not be in compliance. HIPAA requirements are so complex that it is almost impossible to cover everything without your policies and procedures going into great detail.

• Not updating your business associate agreements (BAAs). The BAA you came up with years ago, when associates were first a concern, will not suffice now that HITECH has changed the definitions and relationships with covered entities. ■

OCR not auditing enough providers, OIG says

If you feel like government regulators are breathing down your neck about Health Insurance Portability and Accountability Act (HIPAA) compliance, some of their bosses are thinking just the opposite. A report issued recently by the Department of Health and Human Services Office of Inspector General (OIG) concluded that the Office for Civil Rights (OCR) is not doing enough to enforce the HIPAA Security Rule.

According to the OIG, OCR had not assessed the risks, established priorities, or implemented controls for its Health Information Technology for Economic and Clinical Health (HITECH) Act requirement to provide for periodic audits of covered entities to ensure their compliance with Security Rule requirements. In addition, OCR's Security Rule investigation files didn't contain required documentation supporting key decisions because its staff didn't consistently follow OCR investigation procedures by sufficiently reviewing investigation case documentation.

OIG also found that OCR had not fully complied with federal cybersecurity requirements for its information systems used to process and store investigation data. *(The entire OIG report is available online at http://tinyurl.com/ojzv3xl.)*

The OIG also makes clear in the report that HIPAA compliance audits will continue. The pilot audits OCR ran in 2012 indicated that covered entities generally have more difficulty complying with the Security Rule than other aspects of HIPAA, the report says, and that small covered entities struggle with HIPAA compliance in each of the assessment areas: privacy, security and breach notification.

In a hint of what covered entities might see from OCR this year, the OIG report recommended that OCR take these steps:

• assess the risks, establish priorities, and implement controls for its HITECH auditing requirements;

• provide for periodic audits in accordance with HITECH to ensure Security Rule compliance at covered entities;

• implement sufficient controls, including supervisory review and documentation retention, to ensure policies and procedures for Security Rule investigations are followed; and

• implement the NIST Risk Management Framework for systems used to oversee and enforce the Security Rule.

OCR responded to the OIG report by generally agreeing with the OIG's recommendations and describing how it had already taken action to address them. As for continuing the compliance audits, OCR's response said that future audits "are less likely to be broad assessments generally across the Rules and more likely to focus on key areas of concern for OCR identified by new initiatives, enforcement concerns, and Departmental priorities." ■