Healthcare Risk Management™

August 2011: Vol. 33, No. 8
Pages 85-96

IN THIS ISSUE

Enclosed in this issue:

- ***Legal Review & Commentary:*** Failed coiling procedure; Failure to timely diagnose leads to permanent blindness
- ***HIPAA Regulatory Alert:*** Access report provision in the proposed rule; 12 steps to prepare for an OCR investigation; Daily $100,000 data breaches; Are your doctors ready for 2010? Interim final rule to standardize electronic transactions

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.

AHC Media

Risk managers/compliance officers: Is it possible for us to get along?

Good relationship possible if you avoid turf battles

Compliance officers have taken on increasingly important and visible roles in healthcare organizations, and that role can lead to ruffled feathers when that person and the risk manager disagree on their authority and responsibilities. The result, too often, is an internal spat that prevents either party from doing their jobs well and exposes the provider to liability.

It doesn't have to be that way, says **Roy Snell**, CHC, CCEP, CEO of the Healthcare Compliance Association (HCCA), a professional group for healthcare compliance officers in Minneapolis and a former Mayo Clinic administrator, consultant and compliance officer. Snell has seen that kind of turf battle and says it can be avoided by having the parties clearly understand how their roles are different.

Despite the fact that some risk managers are saddled with compliance duties in their organizations, compliance and risk management aren't just two terms for essentially the same thing, he says.

"For these people to work well together, they have to understand the difference between a compliance risk assessment and a non-compliance risk assessment," Snell says. "Risk managers traditionally study risks to the company: losing investments, fire, lawsuits, things that will cause trouble to the company. Compliance officers look at the risk of what trouble the organization will cause to others, and they shouldn't be spending any time on risks to the company other than the penalties assessed by breaking the law or being unethical."

EXECUTIVE SUMMARY:

Risk managers and compliance officers can clash over their related duties and responsibilities, but delineating each person's role can avoid most problems.
- Failure to work cooperatively can expose the organization to legal and regulatory liability.
- The roles focus on different types of risk.
- Communication before a conflict arises can improve collaboration.
- A proactive approach is best for creating a good working relationship.

A problem can arise when the risk manager insists on being responsible for risk assessments but misses the risks posed by the company to others, Snell says. By the same token, the compliance officer should not be involved with internal risks no matter how hot the topic or how much the compliance officer feels skilled in that area, he says.

"Risk managers should not be offended if the compliance officer conducts a risk assessment on their own," Snell says. "It's all about what risks you're assessing. The government expects compliance officers to do risk assessments. Given the fact that we are the most fined industry in the history of planet Earth because we have not adequately dealt with regulatory and ethical issues, people with turf problems should go away."

Compliance officers' turf battles aren't always with risk managers, Snell points out. He recalls a time when he was a compliance consultant and needed to conduct an audit of a hospital's program. The head auditor at the hospital said he should do it himself because he had performed compliance audits for 20 years. When asked exactly what he had been auditing, the man replied that he had been auditing timecards and looking for vendors who double billed the hospital.

"If the auditor who is only looking for threats to the company says 'this is my turf,' then that organization is in big trouble," Snell says. "The CEO only wants to hear about the money being stolen from the company, and they don't want to hear about problems you're causing others. That attitude is what led the press, the public, and politicians to be fed up and insist on more compliance programs."

Failure to work well together can threaten the success of both offices and lead to more liability in both areas, Snell says. *(See the story on p. 87 for more on the risk of increased liability.)*

Proactive approach is best

So how do the two parties define their turf? Communication is the key, says **Charla Prillaman,** CPCO, CPC, CPC-I, CCC, CEMC, CPMA, CHCO, southeast regional director for AAPC Physician Services, a company in Salt Lake City that provides education and professional certification to medical coders. Compliance is a significant part of coder education, and Prillaman has seen turf battles arise because risk managers and compliance officers never clearly defined their roles.

"Both people need to understand that they serve an important role for the company, and if they don't work well together, that won't equal a good business plan," she says. "You can take great care of your patients and avoid lawsuits, but if you don't follow all the regulatory rules, you're out of business. If you obey all the regulatory rules and fail to provide patient safety and good medicine, you're out of business."

Prillaman recommends that the risk manager and compliance officer should acknowledge the potential for overlap and disagreement, and she says that they

Healthcare Risk Management® (ISSN 1081-6534), including HRM Legal Review & Commentary™, is published monthly by AHC Media, a division of Thompson Media Group LLC, 3525 Piedmont Road, Building Six, Suite 400, Atlanta, GA 30305. Telephone: (404) 262-7436. Periodicals Postage Paid at Atlanta, GA 30304.

POSTMASTER: Send address changes to Healthcare Risk Management®, P.O. Box 105109, Atlanta, GA 30348.

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., one year (12 issues), $499. Add $17.95 for shipping & handling. Outside U.S., add $30 per year, total prepaid in U.S. funds. For approximately 15 CE nursing contact hours, $545. 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.)

AHC Media 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.

Editor: **Greg Freeman**, (770) 998-8455.
Executive Editor: **Joy Daughtery Dickinson** (229) 551-9195 (joy.dickinson@ahcmedia.com).
Production Editor: **Kristen Ramsey**.

Editorial Questions
For questions or comments, call Greg Freeman, (770) 998-8455.

should sit down to discuss solutions before problems arise. A calm, proactive approach will be better than trying to hash out the problems in the midst of a crisis or a high priority task.

"They're not really at odds, but sometimes it feels that way," Prillaman says. "In the heat of an argument, it's easy to say that it's more important not to kill our patients than to make sure we don't overbill. That sounds good at the time, but in the end, both sides of this equation are important. Try not to denigrate the other person's position just because you feel passionate about your own."

One important issue is terminology, Prillaman says. Sometimes the two parties can be using the same terms such as "reducing risk" but mean different things. It can sound as if you're on the same page, when actually you're not, she says. Take the time to define terms, and be willing to hear what concerns the other person has. Work out ways to avoid conflicts.

See other person as a resource

Different backgrounds are one reason that the two parties can butt heads, notes **Vickie Patterson,** CPA, CIA, CHC, an associate director with the healthcare practice of Protiviti, a consulting company in Tampa, FL. Risk managers often come from a nursing background, for example, which gives them reason to stand their ground when discussing clinical issues with a compliance officer who has a financial or legal background.

"Recognizing those differences and seeing them as resource points, rather than reasons to clash, can make a big difference," Patterson says. "The fact is that your backgrounds and skill sets might be very different, but you can both use that to your advantage by calling on each other for assistance with your own investigations. See the other person as a potential benefit rather than writing them off as not knowing what you know."

The differences in the two roles are why **Timothy E.J. Folk,** a producer with The Graham Co., a healthcare consulting company in Philadelphia, always recommends that they be held by different people. Particularly in larger organizations, it is difficult for one person to take on both roles and do them well, he says.

"There are regulatory bodies and sub-bodies, and new regulations and rules coming out every day that the compliance officer has to stay on top of," he says. "Meanwhile, the risk manager has to focus on the safety committee, the physical plant, claims and loss control, and coverage for claims. There's overlap but also very different concerns."

Folk also notes that understanding the compliance officer's duties, and particularly how they are different from your own, can work to your benefit if the organization ever looks to eliminate one of the positions for financial reasons. *(See the story on p. 88 for more on that possibility.)*

For the benefit of the provider and the risk manager's career, Snell says risk managers and compliance officers must make a concerted effort to work well together. It is not enough to decide that you will have a good attitude and work well with the compliance officer, he says. A proactive approach to collaboration is needed, he says. "I acknowledge that there are many who are doing this correctly, but there are many who are doing it poorly, and it is hurting all of us," he says. "To get the government to go away and focus their enforcement efforts on some other industry, we have to overcome the problem of those who are doing it poorly."

SOURCES

Timothy E.J. Folk, Producer, The Graham Co., Philadelphia. Telephone: (215) 701-5231. Email: tfolk@grahamco.com.
Vickie Patterson, CPA, CIA, CHC, Associate Director, Healthcare Practice, Protiviti, Tampa, FL. Telephone: (813) 348-3407.
Charla Prillaman, CPCO, CPC, CPC-I, CCC, CEMC, CPMA, CHCO, Regional Director, Southeast, AAPC Physician Services, Salt Lake City, UT. Telephone: (800) 200-4157 Ext. 310. E-mail: charla.prillaman@aapcps.com.
Roy Snell, CHC, CCEP, CEO, Healthcare Compliance Association, Minneapolis. Telephone: (952) 933-8009. E-mail: roy.snell@corporatecompliance.org. Web site: www.hcca-info.org. ■

Turf wars can create liability for hospitals

A poor working relationship with the compliance officer can lead to more than just frustration and the occasional argument, cautions **George B. Breen,** JD, an attorney with the law firm of Epstein Becker Green in New York City. It also could lead to substantial liability for the healthcare provider.

A compliance officer and risk manager who do not work well together can inadvertently trample on each other's investigations and put sensitive information at risk of disclosure, he says. For that reason, consider whether certain problems should be the purview of one party or the other, he says.

It is only natural for the risk manager to want to

take ownership of some issues that involve defending the organization from claims brought by a third party or by an employee, Breen says. Sometimes, however, the risk manager's proper role is to contribute but not necessarily to take the lead, he says. "The risk manager certainly can be valuable in helping protect the organization in this instance, from this particular threat, but the compliance officer may also be conducting a broader investigation that ultimately gets turned over to the government as part of a voluntary disclosure," Breen says. "The way you conduct the investigation, with that eventual outcome in mind, may be very different from the way the risk manager would conduct it with different concerns in mind."

Conversely, clumsy interference from the compliance officer can compromise information that the risk manager gathered as a part of a work product or otherwise privileged investigation, Breen says. The difficulty in sharing some privileged information is one reason some providers see a benefit to having one person take on both roles, he says.

For example, Breen says, the risk manager might be alerted to a potential claim arising from the care of a patient. An investigation uncovers a potential flaw in the system, a way that the injury could have been avoided. That information is important for the defense of the malpractice case but might be privileged, yet the compliance officer should be alerted to this potential problem so that he or she can address it from the compliance perspective.

"You don't want the compliance side to lose the ability to benefit from the information gathered on the risk management side," he says. "At a minimum, these two parties must work collaboratively, but even that will not eliminate dilemmas of sharing privileged information. But it's a certainty that a poor relationship will only worsen the problem and expose the organization to far more liability."

SOURCE

George B. Breen, JD, Attorney, Epstein Becker Green, New York City. Telephone: (202) 861-1823. E-mail: GBreen@ebglaw.com. ■

Working well together is good for your career

A good working relationship with the compliance officer will not only avoid squabbles over turf but actually enhance the productivity of both offices, says **Timothy E.J. Folk,** a producer with The Graham Co., a healthcare consulting company in Philadelphia.

For example, the compliance officer can communicate information from his or her field, such as data reported in the development of a regulation, that information can help the risk manager improve safety programs or clinical protocols. Likewise, the risk manager can inform the compliance officer about insurance coverage that might be required before signing a contract with a funding source.

"That's the kind of give and take you want to see," Folk says. "You have certain skills and information, and so do I, so let's work together and do the best we can for this company."

Cooperation can only benefit the risk manager in the long run, says **Joseph W. Dorr,** MS, CIH, CSP, a safety consultant with The Graham Co. in Philadelphia, who works closely with hospital risk managers. Though Dorr and Folk advocate separate positions, they acknowledge that increasing financial pressure on hospitals could lead some to choose between one or the other, lumping both responsibilities on the same person.

"If that happens, it is your benefit to at least have that 30,000-foot understanding of compliance duties," he says. "We may start to see organizations face the difficult choice of whether to keep both positions or combine them into one, and if you're vying for that role, you will be in the better position if you have worked well with your counterpart and know that job to some extent."

SOURCE

Joseph W. Dorr, MS, CIH, CSP, Safety Consultant, The Graham Co., Philadelphia. Telephone: (215) 701-5250. Email: jdorr@grahamco.com. ■

Joplin tornado shows EHR value in disaster

When an EF-5 tornado, among the biggest ever recorded, hit St. John's Regional Medical Center in Joplin, MO, the damage was so severe that all the patients had to be evacuated and taken to other hospitals outside the community. Their medical records were accessible, however, and the hospital was providing care again within a week, all because the hospital had adopted electronic health records (EHRs) only weeks before

the disaster.

Five patients died when their ventilators failed after power was lost and the emergency generators were destroyed, says hospital spokeswoman Joanne Cox. There were 183 patients in the hospital at the time of the storm. There were 175 staff in the building, and there were no staff fatalities.

After the tornado passed, patients were helped down darkened stairways to the main level where a triage area was set up outside. From there, patients were transferred to other hospitals._

Communication in the community was almost non-existent immediately following the tornado on May 22, says Mike McCreary, chief of services for Mercy Technology Services, which provides technical support for St. John's and other hospitals in the Sisters of Mercy Health System. The hospital's information technology infrastructure was destroyed along with the building. However, less than one week after Joplin was hit by the deadliest tornado in U.S. history, St. John's again was caring for patients.

New system worked

The process of setting up a 60-bed mobile hospital and tracking patients' medical histories has been significantly aided by the newly implemented electronic health record system and by the quick action of re-establishing communications. In April, the Sisters of Mercy Health System opened a state-of-the-art data center for mission critical applications and clinical data for its 28 acute care hospitals across a four-state region.

The new data center, in Washington, MO, is about 250 miles from Joplin and was unaffected by the violent weather. Additionally, that data was backed up at another distant location. Just three weeks before the tornado hit, St. John's went live on its scheduled switch to its new electronic health records system from Epic Systems Corp. in Verona, WI. St. John's was the last major hospital in Mercy's system to go live with EHRs.

With the patient data from the distant location, hospitals accepting the evacuated patients could access the EHRs quickly using the patients' identification bracelets or other records sent with them. The data also allowed St. John's to resume providing care in their stricken community within a short time.

Patient's records accessed

The hospital provides one example of a patient who benefitted from the use of EHRs: Paul Johnson, 78, of Joplin, had been hospitalized with pneumonia for two days when St. John's was hit by the tornado. His family members were visiting at the time of the tornado. After it passed, they helped guide him down a dark stairwell with the light from a cell phone to the makeshift emergency department outside. He was stabilized before moving to a triage center at McAuley Catholic High School. When patients there were transferred, he expressed his desire to go to St. John's Hospital in Springfield, knowing the Mercy connection and that his records would be easily accessible.

"I knew that they would want to know my medications, dosages, and what tests had been done, and I knew that I couldn't remember all of it," Johnson told Cox afterward. "The doctors in Springfield were able to pull up my records and ask me questions. It worked out beautifully."

Communication restored soon

McCreary noted that St. John's patients also have access to historical medical records. More current health information was stored within the new EHR, and older paper records had been scanned prior to the tornado and are securely stored on servers located in other communities.

Along with the quick access to patient records, Mercy was among the first organizations in the area to re-establish communication services such as phone, network access, laptops, printers, etc., which helped provide the critical link between Mercy's command center in Joplin, the new mobile hospital, physician offices in the community, and other locations across Mercy. *(See the story on p. 90 for more on how wireless communications can help after a disaster.)*

The local utilities give priority to restoring

EXECUTIVE SUMMARY:

The recent tornado that hit a hospital in Joplin, MO, demonstrates that an electronic record system can prove beneficial during a disaster. The hospital only recently had adopted electronic records, which were used when the physical records would have been inaccessible.

- The hospital took a direct hit from a major tornado and had to be evacuated.
- By accessing electronic records, the hospital was able to resume care within a week.
- Records were available even though the hospital's technology infrastructure was destroyed.

power and other services at hospitals in a disaster, McCreary says, but it was important for St. John's to have the internal capabilities to act once power was restored.

"If the tornado had hit a month earlier, before installing the electronic health record system in Joplin, St. John's would not have been able to bring up our mobile hospital within a week's time. We still would not be operational at this point," McCreary says. "Today, patients have continuity of care across all of our physician locations and the new St. John's Mercy Hospital, and connection to the entire Mercy health system, because of our EHR and our ability to quickly re-establish communication services."

SOURCE

Mike McCreary, Chief of Services, Mercy Technology Services, Joplin, MO. Phone: (417) 820-2426. E-mail: mike.mccreary@mercy.net. ■

Wireless, laptops can work after disaster

The experience at St. John's Regional Medical Center in Joplin, MO, after the tornado is an excellent example of how electronic health records (EHRs) can improve disaster response if the system is structured correctly, says **Elliot Davis**, internet security officer and director of information technology at Beaumont Health System in Grosse Pointe, MI. The key is to have the data accessible from a distant location, as St. John's did, or on "the cloud," in which data is stored on another company's servers or spread through the Internet, Davis says. *(See the story at right for more on off-site storage.)*

Beaumont's emergency preparations include keeping on hand several laptops equipped for wireless communication. "As long as we have one network connection and some access points, we can start triaging patients very quickly," Davis says. "So not only do we have medical equipment and supplies in the triage tents set up outside in the parking lot, but we also have their medical records there electronically."

The system also allows Beaumont to provide care at a remote location for other reasons, such as patients that should be decontaminated in the field before being brought to the hospital. Davis says EHRs will always be more useful than traditional records after a disaster as long as it is possible to make a network connection to a distant site, which proved possible even in the immediate aftermath of the Joplin tornado. "After a disaster there is a lot of chaos, and if you can get those wristbands into an electronic record system, you can quickly identify what they're here for and hook that up to their EHR. If it is your patient, you get access to their entire medical history quickly," he says. "If you have paper records, you have to bring those out into the parking lot, find the right records, and match them with the person. Then you still have the question of how that record moves through the system with them and how do you update it."

In addition, he says, paper records can get lost in transit, documents can get out of order, and lab results can be lost. *(See the story on p. 91 for potential legal ramifications of not having EHRs after a disaster.)*

"Your clinicians can use essentially the same system they use every day, even if they are standing out in the parking lot after a tornado or if they are out in a field somewhere after a plane crash," Davis says. "We also have a BYOD system — bring your own device — that allows doctors and others to bring their iPads and laptops with them to a disaster. We hook them up to the wireless and they have it with them all the time, so they can focus on caring for patients rather than learning how to do paperwork after a disaster."

SOURCE

Elliot Davis, Internet Security Officer and Director of Information Technology, Beaumont Health System, Grosse Pointe, MI. Telephone: (248) 733-7337. E-mail: EDavis@Beaumont.edu. ■

Remote access, backup key for disaster recovery

Cloud computing can be a lifesaver for healthcare providers recovering from a disaster, says **Bassam Tabbara**, PhD, chief technology officer and co-founder of Symform, a data storage provider based in Seattle.

The term refers to the use and access of multiple servers through a digital network such as the Internet, using various devices with a wireless or wired capability. All the data is stored on these distant servers, the cloud, rather than on your own computer system, Tabbara explains. Off-

site backup systems such as Carbonite or Mozy are examples of cloud storage.

The downside is that cloud storage can be expensive, Tabbara says. Storing two terabytes of data on the cloud could cost $1,000 per month, as opposed to about $80 for storing that same data on physical disks. Symform's method of storage is less expensive than some cloud storage providers because the company uses multiple smaller servers rather than building one large and expensive data center, he says. Users contribute some of their own storage capability for other cloud users, which distributes the load and provides backup, he says.

Reliability is another key concern for off-site storage, says **Chris Haudenschild**, chairman of the board and CEO of CliniComp International, a company in San Diego that provides documentation systems for healthcare providers. He recommends always looking for a system designed so that no single point of failure in the system will make your data unavailable.

"That means no failure of software, hardware, or power can stop the system," Haudenschild says. "By having a redundant system at a distant location, you can still have the complete records even if the hospital itself is leveled."

He suggests that healthcare providers are lagging behind in ensuring that records are accessible after a disaster. Some hospitals still make a backup of data and physically take it to a different location, or send an electronic backup copy to off-site storage. The problem with those approaches is that the data is always out of date.

"The bar has been set pretty low so far," he says. "There has been a lot of focus on electronic records and what they can do for the hospital and for patient care, but not as much on how to carry through with that when your facility is hit by disaster. Having electronic records is a huge step forward for that scenario, but it doesn't guarantee access unless you've planned up front and set the system up in the right way."

SOURCES

Chris Haudenschild, PhD, Chairman of the Board and CEO, CliniComp International, San Diego. Telephone: (858) 546-8202. E-mail: Chris.Haudenschild@clinicomp.com.

Bassam Tabbara, Chief Technology Officer, Symform, Seattle. Telephone: (206) 906-9212. E-mail: Bassam@symform.com. ■

Quick data recovery as standard of care

Improved technology is creating an obligation for healthcare providers to recover patient data soon after a disaster, says **Gary L. Kaplan,** JD, an attorney with the law firm of Thorp Reed & Armstrong in Pittsburgh.

That change means that healthcare providers who lag behind in adopting electronic health records (EHRs), and in structuring their system to provide quick emergency access, could face potential liability for resulting harm to patients, Kaplan says.

"I'm not aware of anyone being sued for failing to have electronic access to records after a disaster yet, but I think that could come," he says. "It is increasingly considered part of the standard of care to have an effective disaster recovery program, and that includes access to vital patient data."

Expectations were different only a few years ago, Kaplan says. When paper records were the norm and EHRs were not a realistic option, the public would not have been as quick to expect access to patient records immediately after a tornado or earthquake, for instance. When hurricane Katrina hit New Orleans, Kaplan notes, several hospitals were total losses, and patient records could not be recovered. "We're getting close to a point where that will not be accepted anymore," Kaplan says. "If a patient dies because key information about the medical history or medication use was unavailable after a disaster, we're likely to see plaintiffs or regulators ask why."

SOURCE

Gary L. Kaplan, JD, Thorp Reed & Armstrong, Pittsburgh. Telephone: (412) 394-7740. E-mail: gkaplan@thorpreed.com. ■

Wrong-site surgery *still* happens 40x/week

The news from the Joint Commission Center for Transforming Healthcare is not good: No matter how much healthcare providers and regulatory bodies stress the need to avoid wrong-site surgery, this sentinel event still occurs about 40 times a week.

That figure was disclosed as the center announced the preliminary results of a wrong-site prevention project with eight hospitals and ambulatory surgery centers (ASCs). The facilities identified the most common causes of wrong-site surgery as scheduling and preoperative/holding processes, ineffective communication, and distractions in the operating room.

The timeout procedure, which held so much promise for eliminating wrong-site procedures when it was first introduced, has been found to be imperfect. Even when the timeout is conducted, not all people in the operating room participate, the facilities reported.

Mark R. Chassin, MD, FACP, MPP, MPH, president of The Joint Commission, said during a news conference that the hospitals' reports were useful in identifying the likely causes of wrong-site procedures throughout the health system. "The eight hospitals and ASCs identified where errors can creep into the process and took steps to correct them," Chassin said. "We hope to use their experience as a roadmap to measure risks."

All facilities and physicians who perform invasive procedures are at some degree of risk, he said. In 2010, wrong-site surgery was the third most common sentinel event reported, he noted. "The magnitude of this risk is often unknown or undefined. Providers who ignore this fact, or rely on the absence of such events in the past as a guarantee of future safety, do so at their peril," Chassin said. "Unless an organization has taken a systematic approach to studying its own processes, it is flying blind."

Because wrong-site surgeries are relatively rare events, they are difficult to study, he noted. Research has shown, however, that there is usually no single root cause of failure. More often, wrong-site surgeries occur as the result of a number of small errors that compound each other and lead to the final mistake, Chassin said.

Marking the incision site should help avoid wrong-site surgery, but the execution varies greatly within facilities, said **Mary Reich Cooper**, MD, JD, senior vice president and chief quality officer of Lifespan Corp., who also spoke at the press conference. Lifespan has four hospitals in Providence, RI, that participated in the wrong-site project. "In the past, the mark was made in the holding area," Cooper said. "We found discrepancies between what was seen there before the surgeon arrived and what he thought he was doing in the operating room. So now we have surgeons go out to the holding area to make the initial mark. Then in the OR before the procedure starts, we affirm that mark, asking if everyone sees the mark. We shut down our OR for a day and put everyone through training. Every new staffer gets the same training."

The type of pen also makes a big difference, she said. "Sometimes, the mark was washed away during the prep," Cooper said. "So make certain that only approved indelible pens are used. This was a simple but important intervention."

Tom Feldman, chief executive officer at the Center for Health Ambulatory Surgery Center in Peoria, IL, noted that timeouts were handled inconsistently in several participating locations. "Was the timeout occurring before prep and drape, or after? Who leads the time out: the circulating nurse or the attending surgeon?" Feldman said. "We closed some gaps and decreased variation. That helps everyone in awareness." ■

EXECUTIVE SUMMARY:

Despite an intense focus in recent years, wrong-site surgery still happens about 40 times per week in the United States. Inadequate data collection and poor execution of timeout procedures are cited as common causes.

- Wrong-site surgery was the third most commonly reported sentinel event in 2010.
- Distractions in the operating room led to some errors.
- Some wrong-site surgeries are the result of multiple errors adding up over time.

Fetal distress delay a common OB claim

Miscommunication among the clinical team and substandard clinical judgment are among the most common causes of patient injury leading to obstetrics (OB) claims, according to "2010: Annual Benchmarking Report, Malpractice Risks in Obstetrics" released recently by Crico Strategies, the medical malpractice company owned by and serving the Harvard medical community in Cambridge, MA.

The company focuses on a data-driven approach to claims management and patient safety, and the report is based on an analysis of more than 800 OB cases from the office setting and the Labor and Delivery unit, from prenatal management to intra- and postpartum care. Most

of these cases name an attending obstetrician who performed a vaginal delivery (or emergency cesarean section) after a prolonged second stage of labor. *(See the story on p. 94 for more on the findings of the report.)*

"Purely from a numbers standpoint, OB cases are still relatively rare. But the emotional, physical, and financial impact on both the patient and the provider is tremendous," says **Gretchen Ruoff**, MPH, CPHRM, program director of patient safety services with Crico Strategies. "So even if you are looking at a relatively small number of cases, it is of critical importance to roll up your sleeves, take a close look, and really understand them so you can take action in your present day environment."

Ruoff cautions that the cases resulting in OB claims are only the tip of the iceberg. A close analysis of those claims will reveal common problems that most likely are affecting many OB patients who escaped injury or for other reasons did not pursue a claim. "You look at the common threads in those OB claims and then look under the surface to see how those are occurring in other cases, too. Then you see that the simple number of OB malpractices can be deceptive, that there is more of a problem than those cases alone," she says.

Most prevalent in the study are cases whose allegations involve mismanagement of second stage labor, operative vaginal deliveries, or prenatal care, Ruoff says. Injuries ranged from the emotional distress of a stillbirth or a severely compromised infant to the tragedy of a maternal death. Analysis reveals that plaintiffs experiencing injuries primarily cite communication failures, judgment lapses, and faulty technique as the reasons behind their injuries and their malpractice cases. *(For the full report, go to www.rmf.harvard.edu. The report will be on the right side of the page. Click on the "Read" icon next to the benchmarking report. For other obstetrics information and guidelines, select "high risk areas" at the top of the page. Then choose "obstetrics.")*

Most perinatal claims in the study cite missteps in judgment and communication during the second stage of active labor, which resulted in delays in the response to fetal distress, Ruoff notes. The most troublesome cases involve failures in clinical judgment fueled by "the loss of individual perspective and the lack of a collaborative discussion," the report says. "Together, these factors hinder obstetrical team members' recognition of fetal distress indicators, especially in a slowly declining situation," the report explains. "Often, the clarity of hindsight reveals that signs of distress were present, but providers isolated in one-on-one labor coaching, or navigating evolving priorities and changing shifts, struggled to maintain the awareness required for accurate decision making.'

The report recommends electronic fetal monitor (EFM) training, followed by regular opportunities for practice, as critical for effective translation of the baby's "language," which can indicate when it is in distress. Interdisciplinary training also is crucial, the report says. *(See the story on p. 95 for more recommendations for how to address common problems found in OB claims.)* "Individuals with strong teamwork skills are less susceptible to loss of perspective, better suited to facilitate action on often-veiled indicators of distress, and less vulnerable to preventable patient harm and allegations of malpractice," the report says. "At the height of expectations, when patient, family, and providers await first sight of the newborn at delivery, fatigue and commotion sometimes diminish preparedness for the unexpected. If unrecognized, these factors can impede the OB team's capacity to make rapid decisions and perform technical maneuvers with the precision necessary to prevent injury to mother and baby."

The report notes that the more severe injuries result from shoulder dystocia. Inexperience, especially with assistive devices such as forceps, vacuum, and dystocia maneuvers, often is identified as the primary reason for alleging negligence in the delivery process. Because complications that require assistive devices and techniques during a vaginal delivery might be infrequent for individual providers, inadequate experience and training

EXECUTIVE SUMMARY:

An analysis by the malpractice insurer for the Harvard medical community shows that delays in treating fetal distress are the most common obstetrics (OB) allegations. Miscommunication among the caregivers is the most common cause of patient injury resulting in OB claims.

- The average payment in OB-related malpractice claims is more than twice that of other clinical areas.
- Sixty-five percent of OB cases involve high-severity injuries, including maternal and infant deaths.
- Drills and simulation-based training, especially with protocols for shoulder dystocia, can significantly improve patient safety.

can increase the risk of such interventions.

Drills and simulations can significantly reduce risk. Units that employ drills or simulation-based training focused on the decision to continue or alter the labor plan might encounter fewer unrecoverable situations and mitigate the dangers of fixation and indecision frequently present in delivery-related claims, Ruoff says. "Risk managers should look at the data in this report and ask if any of this resonates with them, whether some of the issues highlighted here can be found in their own organizations," she says. "Then we advise looking at whether you have enough data to do this kind of analysis of your own experience. Studying your aggregate claims data can reveal the issues particular to your organization and how they rank in prevalence with your OB claims, which may not be exactly the same as in another health system. Then you can investigate whether those problems still exist and how to remediate them."

That approach was the one taken by **Marilyn Owens,** ARM, CPHRM, Director, Risk Management for Cassatt RRG Holding Company, Berwn, PA, a captive insurer of numerous hospitals in Pennsylvania. Owens compared her company's data with that of Crico Strategies, looking for indications that Cassatt might be weaker or stronger in certain areas related to OB cases. "Cassatt is quite comparable in many of the areas, and we're finding that we all seem to have difficulties in the same areas," Owens says. "Communication is really where hospitals need to focus. So many adverse events include communication as a contributing factor, so we are focusing on improving communication and teamwork."

To that end, Cassatt has provided training and simulation equipment to its member hospitals so clinicians can practice emergency drills for shoulder dystocia, maternal hemorrhaging, and other OB emergencies.

"The practicing helps them be able to communicate well and function well if an emergency presents itself," Owens says. "Communication and teamwork is where the support should be."

SOURCES

Marilyn Owens, ARM, CPHRM, Director, Risk Management, Cassatt RRG Holding Company, Berwyn, PA. Telephone: (484) 321-5594.
Gretchen Ruoff, MPH, CPHRM, Program Director of Patient Safety Services, Crico Strategies, Cambridge, MA. Telephone: (617) 679-1312. E-mail: gruoff@rmfharvard.edu. ■

Data: OB payment is twice the average

The report on obstetrics claim from Crico Strategies reinforces some of the facts that make risk managers worry about their OB units. The average payment in OB-related malpractice claims is more than twice that of other clinical areas, according to "2010: Annual Benchmarking Report, Malpractice Risks in Obstetrics" released by Crico Strategies. OB-related malpractice claims averaged $980,000, versus $371,000 for non-OB cases.

One data point does show some improvement, however. In analyzing how often OB patients sue, there used to be a wide disparity among academic and community hospitals, with 2005 data showing 10.9 lawsuits per 10,000 births in academic hospitals versus 5.2 for community hospitals. The most recent data shows those figures almost the same, with 6.0 cases per 10,000 births in academic hospitals and 5.4 in community hospitals.

These are some other findings from the report:

Sixty-five percent of OB cases involve high-severity injuries, including maternal and fetal deaths.

The most common allegations are delay in treatment of fetal distress, cited in 25% of cases at hospitals with more than 2,000 births per year and 19% of hospitals with fewer births per year; improper performance of operative vaginal delivery, cited in 15% and 18% of those groups, respectively; and improper management of pregnancy, cited in 13% and 20% of those groups respectively. The most common contributions to OB claims are substandard clinical judgment (found in 77% of the cases), miscommunication (36%), technical error (26%), inadequate documentation (26%), administrative failures (23%), and ineffective supervision (15%).

Birth asphyxia was the most frequent OB case type, accounting for 27% of cases, and the average indemnity was $1,431,000. The next most common types were shoulder dystocia (18% and $559,000), intrauterine fetal death (6% and $373,000), and maternal hemorrhage (4% and $305,000). ■

Early warning system promotes OB safety

Crico Strategies, the medical malpractice company owned by and serving the Harvard medical community in Cambridge, MA, recommends these remedies for the common causes of obstetrics (OB) claims:

• An early warning system for perinatal adverse event reporting.

To promote safer, high quality care of obstetrics patients, the Harvard-affiliated obstetrics leaders turned to consistent, systematic institutional reporting of six categories of perinatal adverse events:

— maternal death;

— uterine rupture/scarred uterus;

— retained foreign object;

— 5 minute Apgar score ≤ 4, term infant, ≥ 2,500 g;

— brachial plexus injury;

— intrapartum death of a term infant, ≥ 2,500 g; neonatal death of a term infant, ≥ 2,500 g, no congenital anomalies.

Review of these signal data support a proactive effort to facilitate more timely improvements in obstetrical care across Harvard's perinatal units.

• Premium incentives to reward improvement efforts.

Crico-insured obstetricians and certified nurse midwives who regularly participate in a series of patient safety education activities qualify for a significantly less costly malpractice insurance premium category than non-participants. The key requirements: a team training course, study of Crico's OB Guidelines, participation in safety drills, and completion of shoulder dystocia and electronic fetal monitoring CME courses. More than 90% of eligible obstetrical care providers participate.

• OB clinical guidelines to encourage best practices.

Published since 1988 and aimed at the most prominent issues seen in obstetrics-related malpractice claims, the "Clinical Guidelines for the Obstetrical Services of the CRICO-insured Institutions" are a codification of best practices and recommendations of the American College of Obstetricians and Gynecologists, and "Guidelines for Perinatal Care" of the American Academy of Pediatrics.

• Crew resource management.

A structured analysis of 10 years of OB claims indicated that 42% of those cases could have been prevented or mitigated with better teamwork. These data led to the development of Team Performance Plus (TPP), based on the elements of crew resource management, expanded and customized to the unique obstetrics environment. TPP trains to the specific skills of high performance teams: leadership, communication, shared vision, and error-reduction strategies. The program provides the structure and tools needed to effectively implement and sustain those skills, ensure leadership support, and manage roadblocks and resistance. (For more on these remedies and other resources for addressing OB claims, go to www.rmf.harvard.edu and select "high risk areas" at the top of the page. Then choose "obstetrics.") ■

CNE INSTRUCTIONS

Nurses participate in this CNE/ CME 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. 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 e-mailed to you instantly.

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 health care for hospital personnel to use in overcoming the challenges they encounter in daily practice.

COMING IN FUTURE MONTHS

■ Should you disclose another hospital's error?

■ Long-term care liability on the rise

■ Nocturnists improve patient safety

■ Fleet liability and insurance

To reproduce any part of this newsletter for promotional purposes, please contact:
Stephen Vance
Phone: (800) 688-2421, ext. 5511
Fax: (800) 284-3291
Email: stephen.vance@ahcmedia.com

To obtain information and pricing on group discounts, multiple copies, site-licenses, or electronic distribution please contact:
Tria Kreutzer
Phone: (800) 688-2421, ext. 5482
Fax: (800) 284-3291
Email: tria.kreutzer@ahcmedia.com
Address: AHC Media
3525 Piedmont Road, Bldg. 6, Ste. 400
Atlanta, GA 30305 USA

To reproduce any part of AHC newsletters for educational purposes, please contact:
The Copyright Clearance Center for permission
Email: info@copyright.com
Website: www.copyright.com
Phone: (978) 750-8400
Fax: (978) 646-8600
Address: Copyright Clearance Center
222 Rosewood Drive
Danvers, MA 01923 USA

CNE QUESTIONS

5. According to Roy Snell, CHC, CCEP, CEO of the Healthcare Compliance Association (HCCA), what is the key difference between risk managers and compliance officers?
A. Risk managers traditionally study risks to the company, and compliance officers look at the risk of what trouble the organization will cause to others.
B. Risk managers have more of a legal background.
C. Compliance officers typically have better connections with senior administration.
D. Compliance officers usually do not conduct risk assessments.

6. What does George B. Breen, JD, an attorney with the law firm of Epstein Becker Green, say is the likely outcome of a poor working relationship between the risk manager and the compliance officer?
A. Increased liability risks for the organization
B. The elimination of one or both of the positions
C. Intensive oversight by administration
D. Complaints to the Human Resources department

7. What does Gary L. Kaplan**,** JD, an attorney with the law firm of Thorp Reed & Armstrong, say regarding the obligation to provide quick access to patient records after a disaster?
A. He has not seen a lawsuit alleging patient harm for failure to provide access to records after a disaster, but he thinks such lawsuits might come soon, and providers are now obligated to plan for such access.
B. He does not think there will ever be such lawsuits, and the provider is not obligated to provide access after a disaster.
C. There have been multiple lawsuits regarding records access after a disaster, and in each case the plaintiff has lost.
D. There have been multiple lawsuits regarding records access after a disaster, and in each case the plaintiff has won.

8. In the report on OB claims by Crico Strategies, what was the most common allegation?
A. Improper management of pregnancy
B. Errors in medication administration
C. Delay in treatment of maternal hemorrhaging
D. Delay in treatment of fetal distress

Healthcare Risk Management's
Legal Review & Commentary™
A Monthly Supplement

Failed coiling procedure and inadequate follow-up leads to partial paralysis, $23 million verdict

By **Radha V. Bachman**, Esq.
Buchanan Ingersoll & Rooney
Tampa, FL

Barbara Reding, RN, LHCRM, PLNC
Central Florida Health Alliance
Leesburg, FL

News: A 34-year-old nursing student complaining of headaches presented at a local university hospital. Diagnostic testing showed a small aneurysm. During a procedure intended to repair the aneurysm, the woman's brain was pierced. As a result of the inadequately performed procedure and adequate follow-up, the woman is paralyzed on her left side and is in constant pain. A jury found the hospital 100% liable and awarded the plaintiff $17.6 million in damages. A total award of $23.4 million was handed down.

Background: A young mother of four children presented to the hospital complaining of chronic headaches. Tests found a non-bleeding aneurysm in her brain, and a neurosurgeon performed surgery in which coils were inserted into the aneurysm. Counsel for the plaintiff's alleged that during the procedure, the woman's brain was nicked.

By the time the doctors discovered the problem following a longer than reasonable delay, the woman's brain was filled with blood. Significant brain damage had occurred.

Following the procedure, the woman, who had been put on a blood-thinning medication called Heparin, displayed symptoms consistent with a postoperative stroke. The lawsuit filed by the plaintiff contended that a nurse observed the symptoms, but nonetheless continued the medication. By the time doctors discovered the problem following a longer-than-reasonable delay, the woman's brain was filled with blood. Significant brain damage had occurred.

The woman underwent 10 surgical procedures. In one of those procedures, skin from the woman's ankle was moved to the woman's skull, which left her with an ankle tattoo on her head. Additionally, the woman developed Methicillin-resistant Staphylococcus aureus (MRSA), became septic and contracted pneumonia while in the hospital. Since her initial presentation to the hospital, the woman has been hospitalized more than 30 times. Due to her condition, the woman's children have been forced to separate and live in different homes.

The woman uses a wheelchair and is paralyzed on her left side. She suffers incontinence, bladder problems, and urinary tract infections. The woman is unable to work. The woman sued the hospital and the nurse staffing company. The woman's children sought damages for loss of parental guidance, and her

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. **Radha V.Bachman**, guest columnist, have no relationships to disclose. **Barbara Reding**, guest author, has no disclosures.

husband sought an award for loss of consortium.

A jury in the case returned a verdict solely against the hospital in the amount of $23.6 million, allocating $17.6 million to the woman, $1 million to each of the woman's children, and $1.8 million to the woman's husband.

What this means to you: This case exemplifies one of the many high-risk situations that encompass a healthcare risk management program. From the viewpoint of provision of healthcare services, emergency services and surgery, anesthesia, and recovery are but a few of the high risk areas in healthcare today. From a litigation standpoint, the risk also begins with the patient's age and health status. We often expect it is the older patient facing surgical intervention who has the potential to put the organization at greater risk. Consider, however, a 34-year-old female, in apparent good health, mother of four, and a student. Should anything "go wrong" during her hospital course, the healthcare providers circumstantially could be faced with actual damages involving life expectancy dollars, loss of work, loss of activities of daily living functions, and loss of consortium, not to mention punitive damages in the event of a finding of medical malpractice and/or negligence.

It is assumed in this case that an appropriate and properly executed informed consent was obtained prior to the coiling procedure. It is also assumed, by virtue of the definition and regulatory requirements regarding informed consent, the risks, benefits, and alternatives related to this procedure were fully disclosed to and discussed with the patient by the surgeon(s) who would be performing the procedure. The benefits of intervention for a non-bleeding brain aneurysm in a young adult are obvious. The alternatives might include medical/pharmaceutical management and consistent monitoring. The risks would likely include (as most standard informed consent documents today demonstrate) such terms as bleeding, additional unplanned surgical intervention, administration of blood or blood products, rupture, death and more. It is further assumed that the patient was provided the opportunity to ask questions and have her questions answered.

Consent documentation, especially the type that is specific to the designated procedure, aids in the defense of a case and defining whether the occurrence is a reportable event. It is prudent for risk managers to work with their organization to establish consent policies and procedures in accordance with state law, consent definition, and components. Risk managers must work with clinical educators to develop education programs in obtaining and executing informed consent with good documentation of same, to ensure compliance with consent practices.

Informed consent does not stand alone in defending a surgical procedure "gone wrong." The possibility of inadvertently penetrating an area of the brain during the coiling procedure might have been an identified risk in the informed consent process. However, inadequate postoperative monitoring, symptom communication and management, and delayed recognition of presenting symptoms and diagnosis led to failure to rescue this wife and mother before permanent brain and other damage had occurred. This inadequacy raises the ongoing clinical issues of assessment, re-assessment, reporting, communicating, and intervention. Monitoring and interpreting changes in mental and physiological status following the procedure would be critical.

At the heart of this case was the failure to timely diagnose bleeding in the brain and recognize and manage the symptoms associated with it.

At the heart of this case was the failure to timely diagnose bleeding in the brain and recognize and manage the symptoms associated with it. The plaintiff's attorneys alleged "the nurse observed the symptoms" consistent with a postoperative stroke, and the physician continued the heparin orders. Helping the organization understand the importance of assessment, documentation, and hand-off communication, and the need to reinforce and monitor clinical practices, is yet another aspect of the risk manager's role.

While heparin is not the drug of choice for stroke patients, the administration of heparin might have been considered appropriate for some circumstances in a patient presenting with an ischemic (blockage) stroke. It would have been detrimental for a patient presenting with a hemorrhagic (bleeding) stroke. The plaintiff and defense attorneys' expert witnesses most likely argued the positive and negative effects of the continued heparin administration; unfortunately, by the time of trial, this would not and could not change the outcome for the patient. The damage had been done.

The plaintiff and defense attorneys also might have argued the competency of the surgeon(s)

through information obtained via the hospital's peer review and Ongoing Physician Performance Evaluation (OPPE) processes as defined by The Joint Commission. While some of this information is delicately protected, data might be provided to support or refute physician competency. Again, it is important that the risk manager support education programs and requirements for consistent and continuous excellence in safe patient care. Helping others understand why compliance is important is key.

With a tragic outcome such as the one for this patient, an organization must conduct a thorough and respectful analysis of the event. The Centers for Medicare and Medicaid Services (CMS) and The Joint Commission (TJC) require that "the hospital must measure, analyze, and track quality indicators, including adverse patient events" (CMS 482.21) and "conduct thorough and credible root cause analyses" (TJC LD.04.04.05).

Whatever the facts presented at trial, the jury clearly held the hospital solely responsible — for the physicians and surgeons it credentials, the nurses it employs, and the unfortunate outcome for the patient. What does this mean to us? We must be and remain diligent in our efforts to train, lead, and hold accountable all patient safety system practices and procedures. This includes assessment, re-assessment, and communication. We must take the "lessons learned," share them with staff, and clearly identify and implement practices of prevention for the future.

REFERENCE

Florida Circuit Court, Eighth Judicial Circuit, Alachua County, Case No. 01-2008-CA-006413 K ■

Diagnosis delay leads to permanent blindness

$1.8 million verdict rendered

News: A 56-year-old man with complaints of impaired balance and light headedness presented to his local hospital. A resident and attending radiologist interpreted the man's CT scan and read the scan to show old lesions. A physician assistant at the hospital diagnosed the man with vertigo and discharged him with medication. As the symptoms became more severe, the man approached his primary care physician, who completed a more thorough workup. Ultimately, a brain biopsy revealed an intravascular lymphoma. The delayed identification and treatment led to permanent brain damage. The jury entered a verdict against the defendant in the amount of $1.8 million.

Background: Suffering from light headedness and dizziness, an ex-trucker sought treatment at a hospital. A CT scan was ordered, and radiologists reading the scan identified some old lesions. A staff physician's assistant diagnosed the man with vertigo and discharged him with medication and an order to return to his physician for follow-up. Shortly thereafter, the symptoms the man was experiencing became more severe. He went to his primary physician, who ordered an MRI. The MRI revealed that the man had suffered several strokes, and he was subsequently referred to a neurologist for further evaluation.

The man was discharged with an order to seek rehabilitation at a local center. According to the plaintiff's, the neurologist failed to complete a full stroke workup, and the cause of the stroke was not identified at this time.

After presenting to the rehab center, the man's MRI was reviewed again. The man was immediately rushed back to the hospital with an order to test for atypical causes of stroke. During the workup, an intravascular lymphoma was identified. The man was transferred to a larger hospital for treatment, but his charts and slides did not accompany the transfer.

The man allegedly sustained serious and permanent brain damage as a result of the delayed diagnoses. He is now legally blind and unable to walk on his own. Due to the nature of his injuries, the man must reside in a long-term care facility. A lawsuit was filed against the hospital, the radiology group, and various physicians alleging failure to property interpret the CT scan, failure to administer adequate follow-up care, failure to refer the patient to a neurologist, failing to order adequate testing for atypical causes of stroke, failing to obtain brain biopsy, and failing to timely transfer the biopsy results for treatment.

Only claims against the hospital, the radiology group, and the attending radiologist went to the jury. Jurors returned a verdict finding the hospital 100% liable for the man's injuries and awarded damages in the amount of $1.8 million. The judge confirmed the verdict and also ordered the hospital to pay $891,145 in interest.

What this means to you: This case, similar to the other in terms of failure to diagnose or rescue, also led to permanent brain damage in a patient. It involved blindness and the inability to walk independently for a 56-year-old male. The patient, previously employed as a truck driver, is now residing in a long-term care facility for the remainder of his life due to injuries sustained.

Intravascular lymphoma, also known as malignant angioendotheliomatosis is a large cell lymphoma found in the blood cells of the skin and central nervous system. It is known to be rapidly fatal, and the primary treatment for this condition is polychemotherapy.

In the case of this 56-year-old, opportunities existed for an earlier rather than later diagnosis, and those opportunities were missed. Beginning with the initial CT scan following his complaints of impaired balance and lightheadedness, the radiologists identified what they thought to be "old lesions." An opportunity existed to further explore, through the patient's medical history, symptomology, and additional diagnostic studies, the acute or chronic status of the lesions. Instead, a physician assistant (PA) subsequently made the diagnosis of vertigo, prescribed medication, and recommended follow-up with the patient's primary care physician (PCP). There is no indication of an emergency department (ED) physician reviewing or confirming the PA's diagnosis, or of the CT scan results being sent to the patient's PCP. As the patient's symptoms worsened, the PCP ordered an MRI.

In the case of this 56-year-old, opportunities existed for an earlier rather than later diagnosis, and those opportunities were missed.

The clock is ticking; time is brain. Given the MRI result of the evidence of multiple strokes, the PCP referred his patient to a neurologist. The neurologist allegedly failed to implement a full stroke workup (opportunity missed), and a cause of the lesions and strokes were not identified or questioned. This was another opportunity missed. The clock continues to tick. Rehabilitation for the balance impairment and lightheadedness was ordered, and the patient complied. It was only after presentation to the rehab center that the MRI was again reviewed and recommendations made to test for other possible causes for the strokes. Another opportunity for a more rapid diagnosis also was missed when the charts and slides did not accompany the patient to the larger hospital.

Given the patient's ultimate diagnosis, the prognosis might have remained poor, but the physical complications of blindness and the inability to walk independently might have been averted or postponed through medical management of the appropriate diagnosis. Time, in the form of a missed diagnosis, worked against what could be a reasonably successful or, at minimum, comfortable outcome.

What is interesting in this case is the jury's decision and award. The radiology group and the attending radiologist were included with the hospital as defendants before the jury; however, finding only the hospital liable indicated the jury viewed the total responsibility for the provision and administration of healthcare services to rest solely upon the healthcare organization. In addition to the verdict, the judge ordered the hospital to pay interest. The jury's finding of 100% liability on the part of the hospital implies several possibilities: the radiology group and radiologist were found to be innocent of the claims filed against them, they were considered to be employed by the hospital, the hospital's credentialing process was an issue, or the leadership of the hospital was held accountable for the actions of those who provide care within their organization.

This case also raises the question of culpability of the ED physician, the PA, and the neurologist. It is conceivable the ED physician, PA, and/or the neurologist might have been originally named in the suit. It is possible documentation did not support their role in causing harm to the patient, or they opted to settle prior to trial.

Documentation, as it always is, would be one of the "make-or-break" factors in this case. Dates, times, results, interventions, and quality assurance would provide evidence of thorough and appropriate patient evaluation and treatment. Based on the verdict, the documentation presented in this case did not support evidence of a timely and accurate diagnosis. Based on the verdict, the jury determined there was a duty to provide care with a subsequent breach of that duty, injury was sustained, and causation was established. As a result, a 56-year-old will spend his remaining time blind, lame, and living in a long-term care setting.

REFERENCE

Superior Court of Massachusetts, Worcester County, Case No. Not Provided ■

HIPAA Regulatory Alert

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

Proposed rule allows patients to view details of health record access

Begin analysis of your ability to meet requirements now

Compliance and regulatory officers have until Aug. 1 to comment on a proposed rule that includes a new accounting of disclosures provision that gives individuals the right to receive a report on who has electronically accessed their protected health information (PHI).

Although healthcare organizations have been required to maintain an audit trail of access to PHI since the implementation of the HIPAA Privacy Rule, and institutions have always been required to provide a report upon request, the proposed rule will be a challenge for some, according to experts interviewed by *HIPAA Regulatory Alert*.

"Under the exiting privacy rule, an individual has a right to an accounting of disclosures of PHI made by a covered entity, and the accounting must be provided to an individual within 60 days of a request," explains **Gina M. Cavalier**, Esq., Partner, Reed Smith in Washington, DC. The proposed rule suggests several changes to the existing rule, including shortening the timeframe for response to a request for an accounting of disclosures from 60 days to 30 days, Cavalier says. "This shortened time-frame may pose challenges, depending on the hospital's current systems for tracking disclosures," she says.

The proposed rule also adds the right to an access report that enables individuals to learn if specific people have accessed their electronic personal health information. "In effect, OCR [The Office of Civil Rights] bifurcated the existing right to an accounting and created two separate rights: accounting and access report," says Cavalier. The right to an access report implements the HITECH Act's mandate that covered entities account for disclosures, including disclosures made for treatment, payment, and healthcare operations, of PHI made though an electronic health record, she says. "The proposed rule has a broader reach and includes uses in addition to disclosures of PHI in a designated record set, not only an electronic health record," she explains. "Moreover, the report must include a description of who has accessed this PHI for treatment, payment, healthcare operations purposes, as well as any other reason."

"Hospitals already have audit trails in place to identify access to a patient's designated record set, but this capability may only apply to the primary system," says **Kate Borten**, CISSP, CISM, president of The Marblehead Group, a privacy and information security consulting firm in Marblehead, MA. "Some feeder systems, such as a lab or registration system, may not be able to provide the audit trails now needed," Borten adds.

Software that identifies users who access patient records is used by many hospitals to produce access audit trails and identify "snoopers," but the proposed rule will require hospitals to produce a report for patients that provides specific information. *(For a list of information required, see story at right)*

Another issue for many hospitals will be related to business associates, Cavalier says. "With respect to

EXECUTIVE SUMMARY

Hospitals have been required to maintain an audit trail of access to protected health information (PHI) since the implementation of the HIPAA Privacy Rule, and organizations have been required to provide a report upon request. However, the new provision of an access report that is included in the Proposed HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act will be a challenge for some providers.

- The access report must give specific information to the patient requesting his or her report, including names of individuals who accessed their electronic PHI.
- The report must aggregate all access, including access by business associates.
- Although most hospitals collect access information, not all systems include feeder or departmental systems.

both accounting and access reports, covered entities [CEs] must be able to quickly obtain relevant information from their business associates," she says. "The logistics associated with coordinating numerous business associates may pose challenges."

Prepare now

Even though the rule is not yet final, Borten suggests that hospital compliance officers start now to prepare.

"Go through the proposed rule carefully, and evaluate your organization's ability to meet the proposed requirements," she suggests. "Put a plan together to address the technological adjustments and process changes that you will need to make."

After the plan is put together, wait for the final rule, she suggests. Re-evaluate your plan to make adjustments that reflect changes between the proposed and the final rules, and then begin implementation, she says.

At this time, the proposed rule sets Jan. 1, 2013, as the date on which individuals have the right to request an access report from organizations that acquired electronic designated record sets after Jan.1, 2009. Organizations that had acquired electronic designated records sets as of Jan. 1, 2009, have until Jan. 1, 2014, to implement processes to provide the access reports.

Also, start talking to your business associates now, recommends Borten. Because the proposed rule refers specifically to designated record sets, carefully review your business associate relationships to identify which business associates have all or part of the information covered by the proposed rule. Work with those associates to make sure they are aware of the proposal for changes related to disclosure accounting and access reports, Borten suggests. "Don't necessarily make the technological changes at this time, but make sure everyone involved has inventoried their capabilities and identified how they will make changes to comply once the rule is final," she adds.

While you are analyzing your compliance readiness, be sure to talk with your information technology vendors as well, suggests Borten. Be sure they are ready to implement changes once the final rule is published, she adds. "There will be time to implement updates and changes, but no one should wait until the final rule to make plans," Borten says.

There already is pushback from some healthcare organizations with complaints that meeting the requirements are too difficult or too burdensome, admits Borten. Even though OCR states in the proposed rule that the access report must include "information that a covered entity is already required to collect under the security rule," the requirements will present a challenge for hospitals that might not be in full compliance with the rule at this time, she says. The rule requires covered entities to record and examine activity in information systems and to regularly review the activity related to information access.

"There has been a disconnect between the security rule regulations and the interpretation of the rule," Borten says. "The rule is often interpreted loosely, and the access log technology often doesn't extend to departmental or feeder systems, such as lab systems."

At this time there are no official government resources available to help compliance officers prepare, but there should be once the rule is finalized, says Cavalier. "However, the OCR, which enforces the Privacy and Security Rules, periodically posts training materials, answers to FAQs, and other resources on its web site," which is located at http://www.hhs.gov/ocr, she points out. "In addition, covered entities may submit comments on the proposed rule, which may include questions or requests for clarifications," she adds. *(See resource box, below, for information on how to access proposed rule and comment.)*

Borten says that even with the policy updates and potential technology changes some organizations will need to implement, "I think access reports are a good thing." If employees know there is a record of access of PHI and that an individual can request the report, there might be fewer cases of internal snooping, she points out.

"Be sure to remind your employees and anyone who may have access to electronic PHI that there is an audit trail that shows access," Borten says.

RESOURCE

To see a copy of the proposed rule and to see information on how to submit comments, go to www.gpo.gov/fdsys. On the right-side navigational bar under "Featured Collections," select "Federal Register." Select "2011," and choose "May 31." Scroll down to "Health and Human Services" and under "Proposed Rules," select "HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act." Comments about the proposed rule must be submitted by Aug. 1, 2011. ■

Know specifics of proposed rule

Unlike the current privacy rule which identifies purposes that might be omitted from disclosure accounting reports, the proposed rule published on May 31, 2011, identifies those purposes for which disclosures must be tracked and reported.

"Listing what must be included in a disclosure accounting is better because a covered entity doesn't have to make their own decision about what is intended to be included or excluded," says **Kate Borten**, CISSP, CISM, president of The Marblehead Group, a privacy and information security consulting firm in Marblehead, MA.

The current privacy rule states an accounting of disclosures of protected health information must include all disclosures except in the case of disclosures made for treatment, payment, and healthcare operations; to the individual; incident to a permitted use or disclosure; per an authorization; and for various public policy and other enumerated reasons, explains **Gina M. Cavalier**, Esq., Partner, Reed Smith in Washington, DC.

"Covered entities will only be required to account for disclosures made in seven circumstances," Cavalier says. "As a general matter, this is likely a smaller universe of disclosures for which a covered entity must account." The disclosures that must be included in a disclosure accounting are:

- an impermissible purpose (unless a breach notice has been provided);
- public health;
- judicial and administrative proceedings;
- law enforcement;
- to avert a serious threat to health or safety;
- military and other government activities;
- workers' compensation.

The proposed rule is also specific about what should be included in the access reports, says Cavalier. An access report must include:

- the date the electronic designated record set (eDRS) was accessed;
- time of access;
- name of the person, if available, and if not, the name of the entity accessing the eDRS;
- a description of what information what accessed, if available;
- a description of the action taken by the user, if available; for example, "create," "modify," "access," or "delete." ■

Free tool assesses privacy risks

Frequent news stories and headlines about the Department of Health and Human Services (HHS) Office for Civil Rights' (OCR) crackdown on covered entities that have reported data breaches or other privacy rule violations increase the importance of continually assessing compliance with privacy and security rules.

A free, interactive toolkit that helps healthcare compliance, privacy, and information security officers assess and mitigate risks within their organizations is available from ID Experts, a Portland, OR-based software company.

The toolkit also offers information to help organizations prepare for OCR investigations. "The biggest challenge is that every OCR investigation is different, and the only way an organization will survive one is if it is completely aware of the potential paths of the investigator and prepared," said **Rick Kam**, CIPP, president and co-founder of ID Experts.

Twelve steps that healthcare organizations can take to prepare for an OCR investigation are:

1. Assign privacy and security responsibility. Ensure accountability for patient privacy with a specifically designated privacy official in your organization.

2. Conduct an annual risk analysis. Carry out an annual risk analysis intended to identify privacy/security risks and vulnerabilities.

3. Address security vulnerabilities. Implement security measures to reduce risks and vulnerabilities identified in most recent risk assessment.

4. Train workforce. Train workforce members including management and volunteers in patient privacy and security requirements, and document evidence of security awareness enforcement.

5. Develop policies and procedures. Develop thorough policies and procedures for safeguarding protected health information (PHI) and for unauthorized disclosure of PHI.

6. Prepare for privacy incidents. Develop procedures and tools for compliant investigation, analysis, and review.

7. Report incidents. Capture and maintain a copy of the incident report that was created/submitted that triggered concern that a potential breach has occurred.

8. Analyze incidents. Develop and document a detailed description of the facts of the incident and the incident risk assessment that you carried out to determine if the incident requires notification to affected individuals and authorities.

9. Document patient notification. Develop and document your notification to individuals affected by the data breach, including all means used to ensure delivery of the notification.

10. Mitigate harm to affected individuals. Describe actions taken to mitigate the harm to individuals/patients affected by the breach.

11. Send notifications to regulators and media. Develop and document your notifications to necessary regulatory authorities including HHS/OCR as well as media.

12. Determine root cause and corrective actions. Determine and document actions to determine the root cause of the incident and to address the root cause with corrective actions.

RESOURCE

To access the free toolkit and checklist, go to www2.idexpertscorp.com, select "Breach Tools" from the top navigation bar. At the next page, scroll down to "OCR Survival Tool," then "Download Tool Here." ■

Survey shows security is not improving

In spite of increased focus on regulatory compliance, a survey of more than 100 information technology (IT) administrators, managers and executives of healthcare organizations reports ongoing data breaches.

The survey, conducted by Boston-based GlobalSign, an accredited public certificate authority, showed that although 56% of IT security teams are spending between 25% and 100% of their workweeks devoted to compliance, breaches that cost organizations as much as $100,000 per incident are happening every day.

Exacerbating the problem is the sheer number of applications and solutions flooding the market that claim to satisfy security and compliance requirements, according to survey respondents. In fact, results revealed that 79% of respondents find that identifying effective tools that can provide both security and compliance is moderately to extremely challenging. ■

Doctors may not be ready for 5010

As the January 2012 deadline for hospitals to convert to HIPAA Version 5010 quickly approaches, a survey conducted by the Medical Group Management Association (MGMA) has found that medical practices are lagging in the race to meet 5010 deadlines. In fact, 45.2% of practices report that they have not yet started implementation or software upgrades.

While 53.4% of the respondents said that they are fully aware of these HIPAA mandates, the majority said that they have not yet scheduled internal testing. Another 84.8% said that they have not yet prepared an impact analysis detailing how this conversion will affect operations.

Of the respondents, 42.9% said that their practice management vendor is geared up to replace or upgrade their system to accommodate the newer version, 34.5 percent said they are not.

Only 9.2% of practices said that they have begun internal software testing and 2% said that they do not plan to start internal testing until after the January 2012 deadline. ■

Standards in place for electronic transmission

The Centers for Medicare and Medicaid Services (CMS) has issued an interim final rule to adopt the first two in a series of "operating rules" that will standardize the HIPAA standards for electronic administrative/financial transactions.

Adoption of operating rules between 2013 and 2016 is mandated under the Affordable Care Act. Under the interim final rule, CMS adopts the Committee on Operating Rules for Information Exchange (CORE) operating rules for the insurance eligibility verification/benefit determination and claim status transactions. CORE is an initiative of the Council for Quality Healthcare, an alliance of health plans and healthcare industry representatives.

Under the CORE rules, the payer will provide additional information, including benefit levels, co-pays, and deductibles, to enable the provider to know the patient's payment responsibility at the point of service.

Under the Affordable Care Act, CMS must adopt rules for eligibility and claims status transactions effective Jan. 1, 2013. Rules for electronic funds transfer and payment/remittance advice transactions must be adopted by July 1, 2012, effective Jan. 1, 2014. CMS must adopt rules for claims/encounters, enrollment/disenrollment, health plan premium payments, and referral certification /authorization by July 1, 2014, effective Jan. 1, 2016.

CMS will accept public comment on the interim final rule through the business day on Sept. 6. To see the interim final rule, go to http://www.ofr.gov/OFRUpload/OFRData/2011-16834_PI.pdf. ■