Healthcare RISK MANAGEMENT

June 2012 | Vol. 34, No. 6 Pages 61-72

Death after leaving ED leads to outcry, but was the hospital in the wrong?

Patient removed by police but dies soon after in jail

A hospital in Missouri is under fire for having a homeless woman ejected from the emergency department (ED) when she refused to leave; the woman died soon after in police custody from a blood clot. Critics allege the hospital is liable, but others say this might be a case in which the hospital met the standard of care and is not responsible.

Twenty-nine-year-old Anna Brown went to the ED at St. Mary's Health Center in Richmond Heights, MO, a suburb near inner St. Louis, complaining of pain in her leg that was so severe she could not walk, according to police. She was examined, but the source of the pain was not determined. The ED discharged her, but Brown refused to leave for seven hours. She sat in a wheelchair and complained that she needed help. Finally, the ED called the police and had her arrested for trespassing.

Police carried Brown out of the ED, and a police surveillance tape shows them depositing her on the floor of a cell. Fifteen minutes later, she was pronounced dead. An autopsy later determined that she died of a blood clot that traveled from her leg. When the Sept. 21, 2011, incident became public six months later, the woman's family criticized the hospital for its alleged callousness and malpractice. The police said they relied on the hospital's assurance that Brown was not in need of care. The hospital released a statement saying the ED staff had properly examined Brown. *(See the story on p. 63 for more on the case and the hospital's response.)*

> *"…the law will make no allowance for the fact that you thought your patient was faking."*

The hospital will be sued if they haven't been already, says plaintiff's attorney **Jeffrey M. Kimmel**, JD, a partner with the law firm of Salenger, Sack, Kimmel & Bavaro in New York City. "And they will end up settling because I don't expect they would want this to go to trial with the videotape evidence and

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. **Radha V. Bachman**, guest columnist, has no relationships to disclose.

such a clear case of a missed diagnosis. They thought she was drug-seeking, and they were wrong," Kimmel says. "The examination for her complaint was straightforward and obvious, but apparently they didn't do it. Unless the facts are otherwise, I don't see how it will be hard to prove the hospital's liability."

Kimmel said he does have some sympathy for the hospital because EDs must contend with many patients who are malingering, seeking drugs, or otherwise difficult. His advice is to single out those patients for extra attention, rather than trying to get them out of the ED, a solution he acknowledges can be difficult to carry out. "The ED must actually go over and beyond with these patients they suspect are crying wolf or drug-seeking. These are the ones where the diagnosis can be missed, because maybe you've seen this person a hundred times and you know he just wants drugs, so you don't take it seriously and do a proper examination," Kimmel says. "From a human standpoint, that's kind of understandable. But the law will make no allowance for the fact that you thought your patient was faking."

Another plaintiff's attorney says the case will hinge on exactly what care Brown received while in the ED. If she was examined in a manner that meets the standard of care for a patient with her complaint and symptoms, the hospital fulfilled its obligations under the Emergency Medical Treatment and Labor Act (EMTALA), says **Sidney Schupak**, JD, a partner with the law firm of Ashcraft & Gerel in Alexandria, VA.

The protocol for examining a patient with leg pain is clear, Schupak says, so the hospital will need to produce a medical record that shows compliance. "The message here is that status doesn't matter when it comes to EMTALA and negligence," Schupak says. "Sometimes drug-seekers and mentally ill people have medical conditions. They can be the most annoying patients, but the law requires that you overcome that and give them the same standard of care as anyone else."

Schupak points out, however, that it is entirely possible the hospital met the standard of care and her subsequent death was not due to negligence. From a legal standpoint, such cases are fact-specific, and litigation would focus on the exact nature of Brown's symptoms and complaints at the time she was examined.

Executive Summary

The subsequent death of a woman who was ejected from a hospital emergency department has prompted criticism of the hospital. The death might have been unavoidable.

- ✦ The hospital is likely to be sued, attorneys say.
- ✦ The case gained national attention.
- ✦ The hospital claims it properly examined the woman and is not liable.

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.

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.

Executive Editor: **Joy Daughtery Dickinson** (229) 551-9195, (joy.dickinson@ahcmedia.com), Production Editor: **Kristen Ramsey.** Senior Vice President/Group Publisher: **Donald R. Johnston.**

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.)

Editorial Questions

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

The risk manager's first question on hearing of the death should have been whether the patient was assessed properly, Schupak says. If she was and there was no evidence of an embolism, it was proper to discharge the patient, and the death was not the hospital's responsibility, he says.

"The fact that she died of a pulmonary embolism soon after leaving the hospital doesn't mean it should have been caught. It depends on her presentation at that time," Schupak says. "The opposite is possible as well, and she could have had clear signs of an embolism. It all depends on what is in the medical record."

Despite the extensive media coverage of Brown's death and the accusations against the hospital, **Robert Wild**, JD, a partner with the law firm of Garfunkel Wild in Great Neck, NY, cautions risk managers not to rush into changing ED policies and procedures.

"Sometimes drug-seekers and mentally ill people have medical conditions."

"I don't believe there is a systemic problem of hospitals not recognizing and appropriately treating emergency patients. Some conditions can be missed for good reason, and I don't think this case points to any great failing by our hospitals," Wild says. "The real lesson for hospitals may be more about how a story like this can be sensationalized in the media and the damage it does to the hospital's reputation, whether they did anything wrong or not."

SOURCES

- **Jeffrey M. Kimmel**, JD, Partner, Salenger, Sack, Kimmel & Bavaro, New York City. Telephone: (212) 267-1950. Email: jkimmel@salsack.com.
- **Sidney Schupak**, JD, Partner, Ashcraft & Gerel, Alexandria, VA. Telephone: (703) 931-5500.
- **Robert Wild**, JD, Partner, Garfunkel Wild, Great Neck, NY. Telephone: (516) 393-2222. Email: rwild@garfunkelwild.com. ✦

Hospital: Patient treated properly in ED

An autopsy determined that Anna Brown's death in a jail cell in September 2012 was caused by blood clots that formed in her legs and migrated to her lungs, according to authorities in St. Louis, MO. Police say Brown went to three hospitals complaining of leg pain in the days leading up to her death, including her visit to St. Mary's Health Center that led to her arrest for trespassing.

She was wheeled out in handcuffs after a doctor said she was healthy enough to be locked up. The St. Louis Post-Dispatch obtained the hospital's surveillance video that shows Brown being removed from the hospital and the jail's surveillance video of her being put in a cell. The video can be seen at http://tinyurl.com/c6ehyjy.

Kate Becker, president of St. Mary's Health Center, released a statement that said, "We are deeply saddened by the loss of Ms. Anna Brown. Although we are bound by federal patient privacy laws and can't share the specifics of this situation, it's important for our community to know key facts. We want to assure the public that we did provide care for Ms. Brown. We followed established medical guidelines and performed appropriate tests. Unfortunately, even with appropriate testing using sophisticated technology, blood clots can still be undetected in a small number of cases.

"The staff at St. Mary's has heard the outrage being expressed about this tragic event. As a mission-driven organization, we strive every day to serve people who come to us with needs that we as a community have too long neglected. Like you, we search for answers. The sad reality is that emergency departments across the country are often a place of last resort for many people in our society who suffer from complex social problems that become medical issues when they are not addressed. It is unfortunate that it takes a tragic event like this to call attention to a crisis in our midst." ✦

2 HIPAA breaches show continuing weaknesses

Continuing reports of security breaches resulting in the loss of sensitive patient data show the weaknesses of some healthcare organizations, and some experts say criminals are targeting healthcare for cyber attacks.

In one particularly bad loss of data, a Utah Department of Technology Services computer server in Salt Lake City that stores Medicaid claims data was the target of a deliberate cyber attack. In addition to Medicaid clients, the breach also involved information from Children's Health Insurance Plan recipients. The Utah Department of Health reports that the hackers stole the Social Security numbers of an estimated 280,000 Medicaid beneficiaries and made off with less-sensitive personal information of an additional 500,000 individuals.

Howard University Hospital in Washington, DC, recently sent noti-

Executive Summary

Recent thefts of patient data underscore the need to protect laptops and servers. The thefts might indicate that medical information is an increasingly attractive target for criminals.

- ✦ A cyber attack in Utah affected the sensitive information of up 780,000 patients.
- ✦ Data was lost when a hospital's contractor violated rules by putting files on his personal laptop.
- ✦ Complying with government requirements for data security is not enough.

fication to 34,503 patients notifying them of a potential disclosure of their protected health information that occurred when a former contractor's personal laptop containing patient information was stolen. The data included Social Security numbers and financial information.

The laptop was stolen from the former contractor's vehicle, according to a hospital statement. The computer was password-protected, but the data was not encrypted, the hospital statement says. Downloading the data to the contractor's laptop was a violation of hospital policy.

The recent spate of healthcare security breaches shows that simply adhering to HIPAA regulations is not enough to protect sensitive information, says **Neil Roiter**, research director at Corero Network Security in Hudson, MA. Compliance should be a result of a comprehensive healthcare security program rather than ensuring that its components comply with government and industry standards, he says.

"The recent Utah healthcare records breach, in which hackers reportedly stole some 780,000 claims, is a wakeup call that simply complying with regulations that are not part of an overall security program can put the organization at serious risk," Roiter says. "The reported explanation on the part of the Utah officials that the stolen data wasn't encrypted — a basic security fundamental — because federal regulations don't require it, attests to this point."

Roiter says there are other aspects of the breach that appear to potentially contradict officials' claims that they have a strong, multi-layered security program in place. In particular, he notes, the reports indicate that a single password controlled access to all the information on the compromised server. Organizations that hold health records must restrict access to only those people that need it to perform their jobs, enforced with strong, multifactor authentication, such as tokens or biometrics. *(See the story on p. 65 for more on restricting access.)*

> *"It's difficult to catch someone who uses legitimate authority to accomplish mischief…"*

The constant reports of healthcare-related data breaches recently are causing growing alarm in the healthcare industry as well as the population in general, says **Joe Santangelo**, principal consultant with Axis Technology in Boston, which provides data security services. There have been more than 400 incidents affecting more than 19 million individuals since 2009, he says, and more than 20% of these have involved business associates. *(See the stories on p. 65 and p. 66 for more on the most common types of data breaches and how to prevent them.)*

"Breaches are now causing contractual issues when inking an IT business associate," he says. "Allocating liability for confidential information to which a service provider had access to and any resulting data breaches is a major cause of concern."

Breaches are having a direct financial impact on healthcare providers, Santangelo says. He notes that Impairment Resources filed for bankruptcy in April 2012 after a break-in at its San Diego headquarters led to the loss of detailed medical information for roughly 14,000 people. Impairment Resources is a national company that reviewed medical records taken on workers' compensation and auto casualty claims for roughly 600 insurance companies and other customers. Also, the Minnesota attorney general brought the first formal enforcement action against a business associate, Accretive Health, a Chicago-based company that provides debt collection and other financial services to healthcare providers, for an alleged violation under the Health Insurance Portability and Accountability Act (HIPAA).

Minnesota Attorney General **Lori Swanson**, JD, is suing the company and alleging that Accretive Health debt collectors allowed themselves to be perceived as hospital employees in order to obtain access and protected health information from hospital patients. Swanson also accuses Accretive of "issuing emergency room employees 'scripts' for conversations with patients that 'can lead a patient or her family to believe the patient will not receive treatment until payment is made.'"

The biggest unknown is how much insider crime goes unreported, Santangelo says. "It's difficult to catch someone who uses legitimate authority to accomplish mischief that might be mistaken for normal activity under ordinary circumstances. No one has ventured to guess the cost of damage insiders really cause."

Santangelo says many organizations have not yet invested in risk assessments, even though the HIPPA and Health Information Technology for Economic and Clinical Health Act (HITECH) requirements have been known for some time. Organizations' leaders believe that they have proper policies in place, but they have failed to test them, especially where business associates are concerned, he says. On top of this problem, the industry is entering a period of uncertainty as it adopts electronic health records more widely.

There are a number of steps that organizations need to take in order to ensure that data privacy is maintained and business viability is not impacted. Santangelo advises taking these steps:

- Monitor network traffic and event logs for unusual patterns.
- Perform a sensitive data analysis.
- Incorporate data de-identification techniques wherever least-use principles would apply, such as in test environments.
- Implement data leak detection and prevention products.
- Evaluate access management processes and procedures.
- Make use of encryption and data masking wherever sensitive data resides.
- Develop a data management and enterprise governance, risk, and compliance framework.

"If your organization does not have staff that is knowledgeable in these areas, consider hiring or employing firms that have experience in the financial industry where this has been a priority for some time," Santangelo says.

Roiter also makes the point that, in any industry, the commitment to data security must come from high within the organization. Security is not simply a tactical or operational task for IT personnel, he says.

"Management must make security a priority and mandate a risk-based program, supported by policies and enforced with strong controls," Roiter says. "Regulatory compliance will flow naturally from a sound security program, as opposed to a compliance-centric approach, which is not risk-based and may leave serious data protection gaps."

SOURCES

- **Neil Roiter**, Research Director, Corero Network Security, Hudson, MA. Telephone: (978) 212-1500. Email: Corero@schwartzmsl.com.
- **Joe Santangelo**, Principal Consultant, Axis Technology, New York City. Telephone: (646) 596-2670. Email: jsantangelo@axistechnologyllc.com. ✦

Encryption, laptop control are vital to security

Encryption would sharply reduce the risk of damage from any loss of data, and widespread use could discourage thieves from trying to access healthcare information, says **Brad Rostolsky**, JD, an associate with the law firm of Reed Smith in Philadelphia who has worked with healthcare providers to ensure data security. Rostolsky acknowledges that encryption can be costly for a large organization.

"Identity theft professionals are becoming more sophisticated, and the Utah situation shows that," he says. "They had a lot of security, and the hackers were savvy enough to find the one weakness in one level of the server access. The role of the security officer is becoming as important as the role of the privacy officer."

Hospitals also should have policies and procedures in place that prohibit or sharply restrict downloading sensitive information to personal laptops, including those of contractors, Rostolsky says. Requiring encryption is one option.

In addition, there should be a policy that requires the removal of protected information from the laptops of any employee or contractor leaving the organization, he says.

"This should be a policy that is explained up front when the person comes to work for you, and they should be required to give you permission to go on their machines and remove any sensitive information," he says. "That also should be part of your dismissal process, having someone from IT access their laptop to confirm they won't leave with your data, as soon as possible."

SOURCE

- **Brad Rostolsky**, JD, Associate, Reed Smith, Philadelphia. Telephone: (215) 851-8195. Email: brostolsky@reedsmith.com. ✦

Privileged accounts can be gateway to breaches

If you examine the rash of recent data breaches, many follow the same distinct pattern, says **Adam Bosnian**, executive vice president of Cyber-Ark Software in Newton, MA. An attacker obtained access to an administrative or privileged account and then used that powerful entry point to take what they wanted.

Are you guarding your privileged accounts closely enough?

In any computer network, the administrative or privileged account is one used by someone with the authority to do more than simply access the data, Bosnian explains. That person might be an IT professional who supports the system or a senior administrator. They — unlike the typical user who can access the data but not do more — are able to increase their own

access or the access of others and do things that might be forbidden to most users, such as downloading large volumes of data.

"Once inside, they leverage the privileged account, or elevate privileges associated with the account, to gain access to additional servers, databases, and other high-value systems only a select few people are actually granted permission to access," Bosnian explains. "The result, as demonstrated in recent breaches, is easy access to millions of sensitive records. This is the same thing that was found in the Utah breach. Hackers were able to bypass the system because a technician configured the server with a weak password, and the attackers elevated privileges from there."

Because these types of privileged accounts can act as a gateway to an organization's most sensitive data and information assets, they have emerged as the primary target for attackers, Bosnian says. They often hack into a privileged account through simple means, such as an easy-to-crack password, spear-phishing (faking the origin of an email to seek unauthorized access), or exploiting zero-day vulnerability (a weakness that is unknown to the system user or the software developer).

"The problem is that privileged accounts are often shared, with passwords that are rarely changed. This remains the great paradox in the world of identity and access management and security in general," he says. "We know that attackers are targeting these incredibly sensitive access points, and yet personal passwords to websites such as Facebook have higher standards of security and strength. Despite controlling access to an organization's sensitive data assets, these shared accounts simply do not have the same security standards applied to them."

Bosnian notes that these vulnerabilities are not limited to the healthcare industry. Auditors from the U.S. Department of Energy recently found similar problems at the Bonneville Power Administration, including 11 servers configured with weak passwords. One had an administrative account with a default password.

"While troubling, reports of this nature are commonplace and are a contributing reason as to why we continually see massive breaches of this nature in the headlines. At some point, businesses across industries need to wake up and understand that privileged accounts and passwords are the no. 1 target for hackers," Bosnian says. "Controlling these access points needs to be a priority."

SOURCE

• **Adam Bosnian**, Executive Vice President, Cyber-Ark Software, Newton, MA. Telephone: (617) 965-1544. Email: adam.bosnian@cyber-ark.com. ✦

Theft of records or media most common form of breach

Stealing paper records or electronic media was the most common type of data breach in healthcare in 2010, according to the Department of Health and Human Services (HHS) "Annual Report to Congress on Breaches of Unsecured Protected Health Information." Losing the records or media was the second most common incident.

Among the 207 breaches that affected 500 or more individuals:

• 99 incidents involved theft of paper records or electronic media, together affecting 2,979,121 individuals.

• Loss of electronic media or paper records affected 1,156,847 individuals.

• Unauthorized access to, or uses or disclosures of, protected health information affected 1,006,393 individuals.

• Human or technological errors, or other failures to take adequate care of protected health information, affected 78,663 individuals.

• Improper disposal of paper affected 70,279 individuals.

The full report can be found at http://tinyurl.com/4x2s4en. ✦

Security improving, but data still vulnerable

Healthcare providers are addressing data security better than in past years, but the challenge also is growing as electronic health records (EHRs) and mobile devices become more common, according to the "2012 HIMSS Analytics Report: Security of Patient Data."

The report is the third installment of a biannual survey of healthcare provider facilities in the United States regarding patient data safety. The survey was commissioned by the information security practice of Kroll Advisory Solutions (previously Kroll Fraud Solutions), a leading risk consulting firm in New York City, in partnership with HIMSS Analytics, a not-for-profit organization in Chicago that promotes data security.

The use of new technologies, in particular mobile devices in the workplace, has skyrocketed, creating new operational efficiencies and security vulnerabilities, the report notes. Particularly with the rise of EHRs, more healthcare providers are entrusting their patient data to third parties, meaning that the scope of patient data security extends far beyond the walls of their own facility, the report says.

In years past, protecting patient privacy was the primary goal for most

hospitals as they strived for compliance under the Health Insurance Portability and Accountability Act (HIPAA), the report notes. But as the industry has moved toward more digital frontiers with an aggressive transition to EHRs and mobile-based devices, "the increase in cyber threats and system vulnerabilities necessitates that privacy and security no longer be treated as separate issues."

Executive Summary

Healthcare providers report that they are improving data security, but the increased use of electronics is posing more problems. Some providers might be focused more on meeting regulatory requirements than ensuring effectiveness.

✦ More than a quarter of survey respondents report a breach in the past year.

✦ Improvements to security programs are driven more by regulations than by breach experiences.

✦ Most breaches were traced to employees.

In 2012, 27% of all respondents to the survey indicated their organization had a security breach in the past 12 months (up from 19% in 2010 and 13% in 2008). Of those who reported a breach, 69% experienced more than one. "The increase is likely due to a more accurate picture of security and privacy than had previously existed within the industry, thanks to more stringent auditing and reporting guidelines," such as the Red Flags Rule and the American Recovery and Reinvestment Act (ARRA) of 2009's Health Information Technology for Economic and Clinical Health Act (HITECH), the report says.

"The positive impact of these changes is that there is a growing level of awareness around the state of patient data security in the U.S. healthcare industry related to increased regulation and the policies put in place to comply with those rules," the researchers write. "However, there is cause for concern, as our new study shows that the security practices in place continue to overemphasize a 'checklist' mentality for compliance without implementing more comprehensive and sustainable changes needed for meaningful improvements in the day-to-day handling of patient Personal Health Information (PHI) and Patient Identity Integrity (PII)."

While increased regulation and better-articulated guidance have led to increases in privacy and security measures within hospitals, they also have contributed to a false sense of security within organizations that comply with these mandates, the report says. "Despite the increase in the number of breach incidents reported, most hospitals continue to believe that if they are more prepared, they are more secure," the report says.

On the whole, individuals responding to the 2012 survey reported they were more prepared than two years ago. Respondents gave themselves a 6.40 on a scale of 1-7 in 2012, compared to 6.06 in 2010 and 5.88 in 2008. That score might indicate confidence in meeting requirements, however, and not necessarily true effectiveness.

"While organizations are actively taking steps to ensure that patient data is secure, they are so focused on meeting compliance requirements that they have little awareness of the efficacy of their security programs," the researchers write.

Ninety-six percent of respondents reported conducting a formal risk analysis at their organization, but 27% reported they had experienced a breach, and 18% were not aware of whether their organization had experienced a data breach in the past 12 months.

Of those who experienced a security breach, only one-quarter said it triggered an update to their organization's security action plan. Instead, 73% said changes in external policies and regulations such as HIPAA and HITECH drove updates to their action plan for securing patient information.

Similar to the studies in 2008 and 2010, respondents were most likely to indicate that breaches at their organizations were caused by an individual employed by the organization at the time of the breach. In 2012, 79% of respondents said that a breach was caused by an employee.

The full report can be found online at http://tinyurl.com/cab93ur. ✦

Background checks useful, but limited

About 73% of employers conduct criminal background checks on all job candidates, according to a 2010 survey by the Society for Human Resource Management, and another 19% of employers do so only for selected job candidates. They can be particularly important in healthcare when a job applicant must be trusted with vulnerable patients and data, but experts caution that background checks have limitations.

Background checks are allowed in almost all states, and some states require checks for some healthcare positions, says **Edward F. Harold**, JD, a partner with the law firm of Fisher & Phillips in New Orleans. The Equal Employment Opportunity Commission (EEOC) does not prohibit their use, but it recently issued new guidance that discourages using background checks too broadly. *(See the story on p. 69 for more on the EEOC guidance.)*

To best use background checks, first make sure to use a reputable company that can access far more information than you would be able to find on your own, Harold says. Remember that

Executive Summary

Criminal background checks can be a useful risk management tool, but their effectiveness is limited. Do not depend on them to detect all criminal history.

- ✦ The Equal Employment Opportunity Commission (EEOC) recently issued new guidelines on using background checks.
- ✦ Use a reputable company to conduct the checks.
- ✦ Have a policy that dictates exactly how the information will and will not be used.

some criminal convictions might not show up in the search because there is no single repository of the data.

Civil offenses also might not show up because some, such as a domestic disturbance resulting in a restraining order, might not be recorded in the criminal record, explains **Sandy Glover**, CEO of Gold Shield Legal Investigations in Ormond Beach, FL, which performs background checks. "I also recommend checking their professional licensure," Glover says. "Are they really a nurse? Is their license in good standing? Credit reports also can be useful if this person is going to be in a position in which they could take advantage of vulnerable people, such as an Alzheimer's patient."

Most employers restrict their searches to convictions, not arrests, because the EEOC has made clear that it sees the use of arrests as highly discriminatory against minorities, Harold explains. *(Some employers are beginning to ask applicants for access to their social media accounts to check for negative information. See the story below for more on accessing social media.)*

Even restricting the search to convictions can have an adverse impact on minorities and men, because they often have more convictions, notes **David Christlieb**, JD, an attorney with the law firm Littler in Chicago. But conversely, a healthcare employer takes a risk by not conducting background checks.

> ***"… it would be simple for a plaintiff's attorney to ask why you didn't know that the person you hired had a shady background and then he harmed a patient."***

"The checks are so common now that it would be simple for a plaintiff's attorney to ask why you didn't know that the person you hired had a shady background and then he harmed a patient," Christlieb says. "If you are not required by your state legislature to do background checks, it is still almost expected in the sense that it has become the standard in healthcare to do this. The real question is exactly how you conduct them and what you do with the information."

No matter how you use background checks, have a policy in place before you start checking.

"You must know what you're checking for, how you're checking, and what you will do with what you find. You have to know beforehand how you will respond to certain findings in a background check," Harold says. "Deciding the first time that information appears will only get you in trouble. Consistency is key to avoid charges of discrimination."

SOURCES

- **David Christlieb**, JD, Attorney, Littler, Chicago. Telephone: (312) 795-3264. Email: dchristlieb@littler.com.
- **Sandy Glover**, CEO, Gold Shield Legal Investigations, Ormond Beach, FL. Telephone: (386) 295-6558. Email: sandy@goldshieldli.com.
- **Edward F. Harold**, JD, Partner, Fisher & Phillips, New Orleans. Telephone: (504) 592-3801. Email: eharold@laborlawyers.com. ✦

No need to check applicants' social media

Some employers are taking advantage of people's tendency to post explicit and sometimes disparaging information about themselves on Facebook and other media by demanding access to those sites before hiring. After incidents in which patient information was posted on Facebook, some healthcare providers might consider monitoring employee sites on an ongoing basis.

Not really a good idea, advises **Edward F. Harold**, JD, a partner with the law firm of Fisher & Phillips in New Orleans.

"The law allows you to ask if you want, but we advise clients not to. You may be taking on more responsibility than you realize," Harold says. "If you have access to his Facebook, but you don't bother to check it for 18 months, and then the employee does something criminal, you could be asked why you didn't see his posts about how he was going to shoot up the place. You had his password, and you could have seen the warning signs."

Demanding access also could drive away otherwise good employees who think it's just too intrusive, Harold says. "Generally, if someone is posting something on social media that has any real bearing on their work performance or trustworthiness, you'll hear about it from coworkers," he says. "It's better to hear about that way than to take on the responsibility of monitoring everyone's social media." ✦

Enforcement guidance targets background checks

Healthcare providers using criminal background checks should take notice of enforcement guidance on employer use of arrest and conviction records in employment decisions. Previous arrests and convictions might not be relevant to the current job application, the Equal Employment Opportunity Commission (EEOC) says in Title VII of the Civil Rights Act of 1964, issued in April 2012 by the EEOC.

The new guidance clarifies and updates the EEOC's longstanding policy concerning the use of arrest and conviction records in employment, EEOC Chair **Jacqueline A. Berrien** said in announcing the update. While Title VII does not prohibit an employer from requiring applicants or employees to provide information about arrests, convictions, or incarceration, it is unlawful to discriminate in employment based on race, color, national origin, religion, or sex. The guidance builds on guidance documents that the EEOC issued more than 20 years ago that explained when the use of arrest and conviction records in employment decisions might violate Title VII.

Unlike previous enforcement guidelines, the new guidance urges employers not to automatically disqualify applicants when criminal records are found, even if the charges or convictions were of a serious nature. Employers should give applicants a chance to explain a report of past criminal misconduct before they are rejected outright, the EEOC says. An applicant might say the report is inaccurate or point out that the conviction was expunged, it might be completely unrelated to the job, or the applicant might show he or she has been fully rehabilitated, the EEOC explains.

The EEOC also recommends that employers stop asking about past convictions on job applications. Additionally, it says an arrest without a conviction is generally not an acceptable reason to deny employment.

The materials for the public meetings held on the use of arrest and conviction records, including testimony and transcripts, are available at http://eeoc.gov/eeoc/meetings/index.cfm. ✦

Hospitals seek 90% reduction in specimen errors in 90 days

Can hospitals see a 90% reduction in mislabeled specimens within 90 days? Some hospitals in South Carolina have, and others are about to find out by trying a new toolkit to prevent mislabeled blood specimens used by a hospital that did experience that huge improvement.

Released recently by the South Carolina Hospital Association (SCHA), the toolkit was built from a proposition that by promoting the "just culture" concept, hospitals can radically reduce errors.

The mislabeled blood specimen is an example of a classic, simple, but potentially tragic error. Blood is drawn from one patient at bedside, but the barcoded identification label of another patient is affixed to the vial, says **David Marx**, father of the just culture concept and CEO of Outcome Engenuity, a Dallas-based management consulting firm that worked with the SCHA to develop and release the toolkit.

"It is not a rare event in our nation's hospitals, occurring as frequently as one out of every 1,000 blood draws," Marx says. "The impact can be disastrous. You're incorrectly diagnosed with a disease you do not have, an unnecessary procedure is performed on you, or you receive the wrong blood in a transfusion, simply because another patient's pre-printed label is affixed to your blood specimen."

The just culture approach is ideal for addressing this problem, Marx says. The problem won't be solved by blaming individuals for errors, he says. "Around the country, hospitals are trying to fix problems by whacking their employees into submission," Marx says. "It's not a good strategy, for the employee or the patients they serve."

Using the just culture method, the toolkit employs a specific strategy for blood collection safety called The Final Check. A nurse at bedside draws the blood, affixes a pre-printed label, and then speaking out loud, in front of the patient, reads the last three digits of the medical record number from the patient's arm band and then from the blood specimen container. For example, the nurse would say "749, 749, confirmed" so the patient could hear.

The process reduced mislabeled blood specimens by 90% at Palmetto Health Richland Hospital in Columbia, SC, where the Final Check was first designed and implemented, says **Lorri Gibbons**, vice president of quality improvement and patient safety at the South Carolina Hospital Association. Similar results were seen at five other hospitals: four in South Carolina, and one in North Carolina.

"The just culture shifts focus from the harm and who to blame, and instead targets the design of the system around the healthcare provider and the behavioral choices of providers in those systems," Gibbons says. *(For more on just culture and avoiding blame, see* Healthcare Risk Management, *December 2009, pp. 133-137.)*

Rather than waiting to discover a mislabeled specimen and then disciplining the nurse or lab technician involved, hospitals would instead focus their employees on the behavioral choices most critical to the safe patient care, Gibbons explains. The hospital

leaders recognize that their staff members cannot be perfect, but that they do have choices to make. With the right system around them and the proper focus on how to label a specimen, healthcare providers could produce much better results, she says.

"We had to show the world that there was a better way," Gibbons says. "We wanted to show nurses and lab technicians that there was indeed a better way to do their work. We had to help them be safe. In doing so, we've created a national best practice for specimen labeling."

The Final Check toolkit, as well as reference videos, is available free of charge at www.thefinalcheck.org.

SOURCES

- **Lorri Gibbons**, Vice President of Quality Improvement and Patient Safety, South Carolina Hospital Association, Columbia, SC. Telephone: (803) 744-3549. Email: lgibbons@scha.org.
- **David Marx**, CEO, Outcome Engenuity, Dallas. Telephone: (469) 222-6880. Email: dmarx@outcome-eng.com. ✦

Hospitals band to reform med mal, cut litigation

Seven hospitals in Massachusetts have begun a major initiative to improve the medical liability system in the state. The new alliance has launched its effort with the release of a Roadmap to Reform, an alternative approach to medical liability intended to improve patient safety, increase transparency, reduce litigation, and cut costs to the health care system.

The alliance contains some of the most notable healthcare groups in Massachusetts, with major teaching hospitals, statewide provider organizations, and patient advocacy groups participating. Beth Israel Deaconess Medical Center (BIDMC), which along with the Massachusetts Medical Society (MMS) had a principal role in the research effort to create the roadmap document, is joined by Baystate Health in Springfield, the largest health care provider in western Massachusetts; Massachusetts Coalition for the Prevention of Medical Errors; Massachusetts Hospital Association; and Medically Induced Trauma Support Services (MITSS), a nonprofit whose mission is to support patients, families, and clinicians who have been affected by adverse medical events.

The Roadmap to Reform proposes a process of Disclosure, Apology, and Offer (DA&O), an alternative to the current tort system, which many health professionals say is inefficient, drives health costs higher, and is unduly burdensome to patients, physicians, and the health care system, says **Alan Woodward**, MD, chair of the MMS Committee on Professional Liability and a past president of the organization. The DA&O approach will be instituted, beginning this year, in seven hospitals in the state to test its feasibility in different practice environments with various insurance arrangements.

"The current approach to medical liability is onerous for both patients and physicians," Woodward says. "It discourages transparency, inhibits communication between caregivers and patients, burdens physicians with excessive premiums, leads to unwarranted lawsuits, and motivates physicians to practice defensive medicine. We can make the approach to medical liability much better for both patients and physicians and stop driving unnecessary costs with a new model that promotes honesty and transparency."

The seven hospitals participating in the initiative include three from the BIDMC health system (Beth Israel Deaconess Medical Center in Boston, Beth Israel Deaconess Hospital — Needham, and Beth Israel Deaconess Hospital — Milton); three from Baystate Health system in Springfield (Baystate Medical Center in Springfield, Baystate Franklin Medical Center in Greenfield, and Baystate Mary Lane Hospital in Ware); and Massachusetts General Hospital.

The seven hospitals specifically were chosen to allow demonstration in various hospital settings and within different malpractice insurance models, explains **Kenneth Sands**, MD, MPH, senior vice president for Health Care Quality at BIDMC. The different settings will make it possible to assess the impact on patient safety, malpractice claims, and overall liability costs, he says.

DA&O programs have been implemented in several settings outside of Massachusetts and have demonstrated success as an alternative to the current tort system, Sands says. Both physicians believe that patients and clinicians will regard the DA&O model as fairer, timelier, and more supportive than the traditional response to adverse events, which is adversarial, stifles the exchange of information, and thwarts efforts to improve patient safety. They also say the model will lead to faster resolution of cases and enhanced reporting of medical errors.

Woodward explains how the DA&O system works: Under the DA&O model, healthcare professionals and institutions and their insurers disclose to patient and families when unanticipated adverse outcomes occur; investigate and explain what happened; establish systems to improve patient safety and prevent the recurrence of such incidents; and, where appropriate, apologize and offer fair financial compensation without the patient resorting to legal action. Such a system will not deny patients the right to bring legal action, but it would make tort claims a last resort. Adverse events in which the provider or institution is deemed to have met the standard of care would be firmly defended.

"The DA&O model, which

has been highly successful at the University of Michigan Health Care System for a decade, is gaining broad support across the nation and is regarded as a successful approach to medical liability reform and patient safety by such groups as The Joint Commission," Woodward says.

SOURCES

- **Kenneth Sands**, MD, MPH, Senior Vice President for Health Care Quality, Beth Israel Deaconess Medical Center, Boston. Telephone: (617) 667-1325.
- **Alan Woodward**, MD, Chair, Committee on Professional Liability, Massachusetts Medical Society, Waltham. Telephone: (781) 893-4610. ✦

COMING IN FUTURE MONTHS

- ✦ Hospital cuts errors 30%, falls 88%
- ✦ When is there a doctor-patient relationship?
- ✦ Avoid the risks of e-prescribing
- ✦ Keep complaints from becoming lawsuits

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. 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 QUESTIONS

1. **Regarding the death of Anna Brown after she was removed from the emergency department at St. Mary's Health Center, which of the following is true?**
   A. Brown refused care offered by the clinicians at St. Mary's.
   B. Brown was identified as a drug seeker and ordered removed without any examination or care.
   C. The hospital claims it provided examination and care according to established guidelines but Brown still died from a blood clot.
   D. The hospital clinicians wanted to provide additional care, but the police insisted on removing Brown from the hospital.

2. **In the recent breach of healthcare data in Utah, what was the healthcare provider's explanation regarding encryption?**
   A. The data was not encrypted, because encryption was impossible with this type of data.
   B. The data was not encrypted, because government regulations do not require encryption.
   C. The data was encrypted, but the attacker found a way to defeat the encryption.
   D. The data was encrypted, but the provider does not know if the encryption was defeated.

3. **Which of the following is true regarding the recent guidance from the Equal Employment Opportunity Commission regarding criminal background checks of job applicants?**
   A. The new guidance urges employers not to automatically disqualify applicants when criminal records are found, even if the charges or convictions were of a serious nature.
   B. The new guidance clarifies that there is no risk in automatically disqualifying applicants when criminal records are found, particularly if the charges or convictions were of a serious nature.
   C. The new guidance encourages employers to consider previous arrests, not just convictions, when considering applicants.
   D. The new guidance discourages employers from using criminal background checks in any way because they can be disproportionately harmful to minorities.

4. **What does Edward F. Harold, JD, a partner with the law firm of Fisher & Phillips, advise regarding monitoring employees' social media sites?**
   A. He advises against it, because you might be taking on more responsibility and potential liability than you realize.
   B. Such monitoring is prohibited by federal law.
   C. The monitoring is generally a good idea, and most employers should do it.
   D. Such monitoring is legal only in 12 states.

Legal Review & Commentary

A Monthly Supplement to HEALTHCARE RISK MANAGEMENT

Failure to admit diabetic patient leads to brain damage, $21.4M verdict

By **Jonathan D. Rubin**, Esq.
Partner
Kaufman Borgeest & Ryan
New York, NY

Christine A. Turiano, Esq.
Associate with Kaufman Borgeest & Ryan
Valhalla, NY

Barbara K. Reding, RN, LHCRM, PLNC
Clinical Risk Manager
Central Florida Health Alliance
Leesburg, FL

News: A 50-year-old diabetic man was transported to the emergency department (ED) twice in 48 hours after being found unresponsive by family. Each time, he was diagnosed with hypoglycemia, stabilized in the ED, and discharged home. He developed severe hypoglycemia 10 hours after his second hospital discharge, and he suffered brain damage as a result. He is completely incapacitated. The patient's sister brought a lawsuit against the hospital on his behalf and alleged negligent care. The jury returned a verdict of $21.4 million. The patient's award was reduced to $19.1 million due to his percentage of fault.

Background: A 50-year-old insulin dependent diabetic man was found unresponsive by family on Oct. 11, 2007. He was transported by ambulance to the ED and suffered a seizure on arrival. His blood glucose level was 14, and 50% dextrose (D50) was administered to treat hypoglycemia. Once his blood glucose level stabilized, he was discharged home with instructions to follow up with his physician in two days. The man returned to the ED on Oct. 13, 2007, after having again been found unresponsive by family. He arrived by ambulance at 9 p.m. and was treated for hypoglycemia. He was administered D50, provided with food, and discharged home at 1 a.m. on Oct. 14, 2007, after his blood glucose level was stabilized. The man went to sleep at 3 a.m. and was found unresponsive by family at 10:30 a.m. He suffered a hypoxic brain injury secondary to hypoglycemia, which resulted in permanent brain damage and the need for 24-hour skilled nursing care.

Given this patient's fragile mental capacity and brittle diabetic history, providers had a duty to evaluate, investigate, plan, monitor, and advocate for this patient.

A lawsuit was filed against the hospital by the man's sister on his behalf. The plaintiff argued that the hospital was negligent in discharging the patient twice without determining the underlying cause of his hypoglycemia. The records did not document a change in diet, insulin, or activity level that could account for the patient's change in condition. Plaintiff also argued that records showed a history of increasingly severe hypoglycemic episodes, causing generalized seizures. Plaintiff contended that repeated episodes of hypoglycemia caused development of "hypoglycemic unawareness," which resulted in the man's higher tolerance for lower glucose levels. As a result, he might not have exhibited typical hypoglycemic symptoms prior to loss of consciousness. Plaintiff additionally argued that the hospital failed to appreciate the patient's history, and the fact that he was taking Lantus (long-acting insulin)

FINANCIAL DISCLOSURE: 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. **Christine A. Turiano**, Esq., **Barbara K. Reding**, and **Jonathan D. Rubin**, co-authors, have no relevant relationships to disclose.

at the time of his presentation to the hospital. In light of the patient's history and unexplained hypoglycemia, plaintiff argued that the patient should have been admitted to the hospital for further work up, or at the least, admitted to the Clinical Decision Unit (CDU) for observation. The CDU is available to observe patients who don't necessarily require hospital admission. Plaintiff also highlighted the refusal of each treating physician to take responsibility for the decision to discharge the patient and alleged that family was never instructed to observe the patient following hospital discharge.

In support of the hospital, the defense argued that it is standard ED practice to treat hypoglycemia by stabilizing glucose levels and by discharging the patient to his primary care physician and family. The defense also focused on the patient's 7-year diabetic history, including weekly and biweekly physician visits for uncontrolled diabetes. The patient experienced blood sugar fluctuations despite multiple medication adjustments. The defense argued that the patient's documented noncompliance was the cause of his fluctuating glucose levels (documented 37 times between 2000 and 2007). The defense also referenced his history of schizophrenia, depression, and daily alcohol consumption. The defense argued that the patient's own failure to take medications as prescribed, follow a proper diet, and avoid alcohol contributed to his repeated development of hypoglycemia. The defense also highlighted the patient's 11 prior hospitalizations for hypoglycemia due to the patient's noncompliance.

The jury returned a verdict of $21.4 million dollars for the damages sustained by the patient. However, the verdict was reduced to $19.1 million, which represented the jury's apportionment of 10% of the causal fault to the patient. At the time of the verdict, defense counsel stated that an appeal would be taken. To date, court records don't reflect that an appeal has been filed.

What this means to you: This case presents interesting views related to risk management and responsibility from the plaintiff and defense perspectives. The defense arguments, although designed to prove patient responsibility and demonstrate the patient's noncompliance with his healthcare regimen, serve instead to emphasize the plaintiff's arguments related to breach of duty. With the duty to care comes the additional responsibility to provide such care in an acceptable manner, one that is consistent with the standard practice of other competent professionals providing care in similar circumstances. It is expected that the same degree or standard of knowledge, skill, and care will be performed and executed by healthcare professionals for all patients under the same conditions. Failure to meet the standard of care results in a finding of liability on the part of the defendants.

In terms of assessment and intervention, when making the decision to discharge the patient to home twice within 48 hours, the healthcare providers failed to consider the patient's history of multiple hospitalizations due to severe episodes of hypoglycemia. They failed to incorporate into their plan of care for this patient the concern of frequent physician office visits related to uncontrolled diabetes, unsuccessful diabetic medication management attempts, and most importantly, the patient's psychiatric diagnosis. Two ambulance runs and two episodes of unresponsiveness within 48 hours should have alerted ED staff to the high risk this patient presented. The discharge planners (physicians, nurses, and case managers) should have considered the second event, if not the first, to be an unsafe discharge at the least. A critical glucose level of 14 with associated seizure activity would warrant close monitoring and observation over time, certainly so in light of 11 prior hospitalizations and a documented history of glucose fluctuations. This recently discharged ED patient presenting once again, via ambulance, in acute distress in such a brief timeframe would warrant the prudent consideration of admitting him to an observation or medical unit. Unfortunately, dollars, budgets, and insurance coverage, or lack thereof, often drive or contribute to risky decisions made by healthcare providers. At greatest risk in today's healthcare economic and financial environment is the patient.

The plaintiff's introduction into the case of "hypoglycemic unawareness" brought a compelling argument to the forefront. A potentially developed tolerance for lower glucose levels, coupled with the patient's diagnosis of schizophrenia, might have diminished the patient's ability to fully understand his disease process and decipher the associated warning signs and symptoms of an impending hypoglycemic crisis. Given this patient's fragile mental capacity and brittle diabetic history, providers had a duty to evaluate, investigate, plan, monitor, and advocate for this patient.

The strengths of this case were found in the plaintiff and defense arguments concerning assessment, intervention, and responsibility. With 10% of the damages assessed against the patient and 90% attributed to the hospital and its team members, the jury affirmed the duty and the responsibility to provide prudent and reasonable care, regardless of patient compliance, to rest primarily on the decisions made by the providers. Even so, it was noted that physicians declined

to accept culpability or responsibility for the discharge decisions that led to the devastating lifestyle change and long-term care needs of this patient.

By virtue of the hospital's choice and decision to provide healthcare to those in need, the duty to care is established and the breach of that duty in this case was evident. The hospital provided temporary-only intervention and minimal consideration of the need for long-term solutions, which resulted in the subsequent injury of brain hypoxia and a substantial verdict for the plaintiff. The plaintiff's award however, will be needed to provide care for the patient for the remainder of his life.

Reference

Campbell v. Temple University Hospital. Court of Common Pleas of Philadelphia County, PA. Case No. 090200546. 2011 WL 2595418. ✦

Hypoxic brain injury in birth yields $144M verdict for teen

News: A woman presented to the hospital for induction of labor on Dec. 1, 1995, and she vaginally delivered a 10-pound, 12-ounce baby girl. The baby was not breathing at the time of birth and had poor tone, seizures, brain hemorrhages, and a fractured left clavicle. She was hospitalized in the intensive care unit for three weeks, and she was diagnosed with profound retardation and cerebral palsy. She is now 16 years old and requires round-the-clock medical care. A lawsuit was filed against the hospital and attending OB/GYN by the child's mother on her behalf. Following trial, the jury returned a verdict of $144 million. Pursuant to the applicable state law regarding present value reductions and statutory caps, that amount was reduced to $40 million. Post-trial motions are pending, and defendants are expected to appeal.

Background: During her pregnancy, the plaintiff gained 70 pounds and developed gestational diabetes. She presented to the hospital for induction of labor on Dec. 1, 1995. Pitocin was administered to induce labor, and the plaintiff was actively pushing for two hours. The baby weighed 10 pounds, 12 ounces upon delivery, and she was not breathing. She had scalp and facial bruising and swelling, poor tone, seizures, and a fractured left clavicle. Her skin was described as appearing purple and black in color, evidencing bruising and trauma. Plaintiff also claimed the child suffered multiple brain hemorrhages. Defendant contended that the child suffered only minor intraventricular hemorrhages, which were not in the actual substance of the brain. The baby was hospitalized in the ICU for three weeks, and she was diagnosed with cerebral palsy and hypoxic-ischemic encephalopathy. She is quadriplegic and requires 24-hour medical care.

Plaintiff argued that the OB/GYN was negligent in failing to accurately assess the baby's size prior to delivery. They asserted that the baby was larger than expected due to gestational diabetes. They said that the diabetes, coupled with the mother's weight gain, should have alerted the defendants to the baby's increased size. Plaintiff further argued that the hospital and OB/GYN were negligent in failing to offer a C-section, which allowed the baby to be crushed in the birth canal during delivery. Additionally, plaintiff argued that the hospital negligently selected, employed, trained, and monitored its employees/physicians.

The defense focused on the child's alleged genetic condition as the cause of her injuries and asserted that no hypoxic event took place during the birth. The venous cord gas reading was normal. Ultrasound, CT, and MRI images of the brain showed no evidence of oxygen deprivation or traumatic injury. Moreover, the images showed that 50% of the child's cerebellum and 33% of her brainstem were not present due to a genetic birth defect. Results from court-ordered blood testing during discovery pointed to a diagnosis of pontocerebellar hypoplasia (PCH), a rare condition which results in lack of formation of the brain, profound retardation, spinal cord atrophy, weak muscle tone, difficulty eating/swallowing, and spastic quadriplegia. There are only a few hundred cases of this condition on record, and the child at issue would be the first to be diagnosed in the United States. The condition is progressive and often fatal in infancy. Defendants also argued that there was no evidence of gestational diabetes, as a three-hour glucose tolerance test was normal. Additionally, they argued that estimated fetal weight, as per the prenatal ultrasounds, did not indicate a need for C-section. They said that the mother's morbid obesity prevented an accurate fetal weight estimate.

Experts included a pediatric neurologist, a pediatric neuroradiolgist, an OB/GYN, and a fetal specialist.

The jury returned a verdict of $144 million. About $13.5 million of that amount represented an award for past and future pain and suffering; however, pursuant to the

applicable state law, non-economic damages were capped at $738,000. The remainder of the award represents economic damages, including 24-hour care for 77 years, and lost earning capacity. The defense filed 10 post-trial motions and contends that healthcare costs should be capped under $2 million, in part, because the child's genetic condition will likely shorten her life span. The defense also has indicated it will appeal the verdict.

What this means to you: This case presents a vivid and horrifying description of a traumatic birth resulting in multiple and permanent injuries. Although defense counsel presented arguments of genetic birth defects, normal glucose tolerance test results, and maternal obesity prohibiting an accurate fetal weight, the jury clearly was sympathetic to the plaintiff, as evidenced by the initial verdict awarding $144 million. The defense arguments were plentiful, sophisticated, and well-researched, but apparently they did not override for the jury the images of crushing birth canal injuries and inadequate prenatal assessments and care. Birth, infant, or child malpractice and negligence cases present some of the highest risks for healthcare organizations as damages and award projections are lifelong, as are care expenses and loss of income. The Jurors in this case concluded that the physician who delivered the baby and the hospital were negligent.

One of the pivotal elements in this case was the mother's 70-pound weight gain during the pregnancy. The weight gain factor alone should have alerted the physician, his staff, and hospital personnel to the increased potential for complications arising during the pre-natal, perinatal, and post-partum periods. Plaintiff's counsel argued that it was the responsibility of the physician and the hospital to determine the baby's size and the need for a C-section due to the mother's diagnosis of gestational diabetes and her significant weight gain. The jury agreed that the failure of the physician and hospital to determine the baby's size and consider a C-section was a violation of the standard of care. There was no question as to injury. Causation was thoroughly argued by both counsels.

The jury agreed that the failure of the physician and hospital to determine the baby's size and consider a C-section was a violation of the standard of care.

Of note in this case, the parents were not parties to the lawsuit; in other words, there was no claim for pain and suffering made on their behalf. Also of note, this case was filed in 2005, 10 years after the plaintiff's birth. What does this mean to you? As risk managers, we always must be mindful of the statute of limitations on cases and remain diligent on those events involving infants and children, where the limitation timeframe differs from other claims of negligence. A Notice of Intent for litigation could arise long after an organization and its risk managers consider the claim potential closed. Investigating well all the facts of the adverse event and maintaining full knowledge of the risks of the occurrence prepares risk and claims managers for the possibility of future claims and/or litigation.

Also of note in this case, the plaintiff argued that the hospital was negligent in the selection, training, and monitoring of its employees and physicians. To reduce the risk of such allegations, it is important for an organization to maintain well-documented education, orientation, and in-service records, personnel files, and evidence of adherence to Centers for Medicare and Medicaid (CMS) and The Joint Commission regulatory requirements and guidelines for competency and credentialing. The organization must demonstrate effective peer review processes and consistent practices for corrective plans of action when a practitioner fails to meet the standard of care. The Joint Commission requires utilization of OPPE (Ongoing Professional Practice Evaluation) and FPPE (Focused Professional Practice Evaluation) to ensure safe and reliable care for patients.

It is difficult to assess the financial impact to an organization of a three-week trial requiring several parties of defense counsel, expert witnesses, and associated court costs. Not only was the verdict in this case financially devastating, but the human resources, time, and energy required and devoted to a case such as this one could place a long-term economic burden on the healthcare providers. The importance of creating and maintaining a culture of patient safety in order to minimize risks for the patient and for the organization must be a top priority.

And what of the plaintiff, destined to require 24/7 care and assistance for the remainder of her life? There is no means of truly assessing the impact for her.

Reference:

Vanslembrouck v. William Beaumont Hospital, et al. Circuit Court of Michigan, Oakland County. Case No. 2006-074585-NH. ✦