HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE SINCE 1979

INSIDE

RELIAS MEDIA

DECEMBER 2019 Vol. 41, No. 12; p. 133-144

Hospital Creates Harm Collaborative to Improve Communication With Executives

Some patient safety issues are so important that risk managers and other safety leaders need direct access to the C-suite so that concerns can be addressed quickly. Helen DeVos Children's Hospital in Grand Rapids, MI, devised a harm collaborative that makes that possible.

The collaborative meets weekly so that risk managers and other safety or quality professionals can address the executive team about individual patient cases or trends that are concerning, says **Laura Bailey**, senior clinical risk manager with the hospital. The collaborative was developed in 2015 by Bailey's predecessor in risk management.

> THE COLLABORATIVE MEETS WEEKLY SO THAT RISK MANAGERS AND OTHERS CAN ADDRESS THE EXECUTIVE TEAM ABOUT INDIVIDUAL PATIENT CASES OR TRENDS THAT ARE CONCERNING.

"It originally was intended as a meeting at which we discussed every single harm event that affected a patient, keeping the leadership team aware of trends so they could improve safety efforts more rapidly," Bailey says. "It has evolved a lot over time so that while we still talk primarily about safety events, it's also a time for us to bring up any major process issues that we see or hear being reported. Maybe we haven't necessarily had a safety issue with it yet, but we have a big cumbersome process that teams are struggling to solve. The executive team can help us escalate the problem so that we get faster solutions."

ReliasMedia.com

Financial Disclosure: Author **Greg Freeman**, Editor **Jill Drachenberg**, Editor **Jonathan Springston**, Editorial Group Manager **Leslie Coplin**, Accreditations Manager **Amy Johnson, MSN, RN, CPN**, 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. Consulting Editor **Arnold Mackles**, MD, MBA, LHRM, discloses that he is an author and advisory board member for The Sullivan Group and that he is owner, stockholder, presenter, author, and consultant for Innovative Healthcare Compliance Group.

HEALTHCARE RISK MANAGEMENT™

***Healthcare Risk Management™*, ISSN 1081-6534, *including Legal Review & Commentary*,™ is published monthly by Relias LLC, 1010 Sync St., Ste. 100, Morrisville, NC 27560-5468. Periodicals postage paid at Morrisville, NC, and additional mailing offices. POSTMASTER: Send address changes to *Healthcare Risk Management*, Relias LLC, 1010 Sync St., Ste. 100, Morrisville, NC 27560-5468.**

GST Registration Number: R128870672

SUBSCRIBER INFORMATION:
Customer Service: (800) 688-2421.
customerservice@reliasmedia.com
ReliasMedia.com

MULTIPLE COPIES: Discounts are available for group subscriptions, multiple copies, site licenses, or electronic distribution. For pricing information, please contact our Group Account Managers at groups@reliasmedia.com or (866) 213-0844. 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.

ACCREDITATION: Relias LLC is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation. Contact hours [1.5] will be awarded to participants who meet the criteria for successful completion. California Board of Registered Nursing, Provider CEP#13791.

Relias LLC is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians. Relias LLC designates this enduring material for a maximum of 1.5 *AMA PRA Category 1 Credits*™. Physicians should claim only credit commensurate with the extent of their participation in an activity.

Healthcare Risk Management™ is intended for risk managers, healthcare administrators, healthcare legal counsel, and physicians.

This activity is valid 36 months from the date of publication.

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.

AUTHOR: Greg Freeman
EDITOR: Jill Drachenberg
EDITOR: Jonathan Springston
EDITORIAL GROUP MANAGER: Leslie Coplin
ACCREDITATIONS MANAGER: Amy M. Johnson, MSN, RN, CPN

EDITORIAL QUESTIONS
Call Editor **Jill Drachenberg**, (404) 262-5508

Bailey collaborates closely with **Heather Githu**, senior safety specialist at the hospital, to determine which safety events should be discussed at the meeting. The risk manager primarily brings events that came through the hospital's event reporting system, which involve patient harm or issues that the executive team should know about.

Simplicity Is Key

The meetings are informal, and executives often refer to it as their "don't miss" meeting of the week because it is so informative, Bailey says. Usually, about a dozen senior executives and safety leaders participate.

Harm collaborative meetings last one hour and rarely are cancelled, Bailey says. Monthly meetings would not be as useful, she says, because incidents from three weeks earlier will not be as fresh in the mind and may be forgotten. Participants also will not remember as clearly what was discussed that long ago.

The simplicity of the meeting is part of what makes it work, she says. "In an informal manner, I'll present the cases, and then we'll open it up for discussion with the team to make sure I've done a thorough investigation, in case there are things I didn't think of but that the senior leaders think need investigation," Bailey says. "We will then talk about next steps, if they are necessary to resolve the problem."

Githu often follows up with trend reports and a recap of her meetings with unit-level leaders and their safety concerns or process issues.

"Any time we do a root cause analysis or an apparent cause analysis, I bring the action items to the harm collaborative and go over those. That's a place where we can get engagement with leadership to address any barriers we think might encounter on those action items," she says. "Also, the executives are more aware of what's happening in our entire health system, so they may be able to tell us that this action item is already slated to be addressed in the near future with a solution. They also may push back on some action items because they want to be sure the solution is really solid, which makes us use strong action items and not just fall into lower levels of effectiveness."

Githu brings the nurses who performed apparent cause analyses so they can speak directly to the executive team about what they found. Bailey also brings in unit-level employees to speak to the harm collaborative because they often can describe the issue more effectively

EXECUTIVE SUMMARY

A hospital developed a process for conveying patient safety issues to executives. The process provides health and safety leaders direct access to the C-suite.

- The risk manager and safety leaders meet weekly with executives.
- Safety events are on the agenda, but so is any process issue that could threaten patient safety.
- The meetings are specifically not for solving problems, but rather for identifying them and possible solutions.

than she can, and answer the questions of the executives.

"It's gotten so that I have managers reaching out to me now to say they know this issue isn't a harm event but they're really struggling with a process and they'd like to come to the harm collaborative to talk to the team about it," Bailey says. "That's a win because it makes the executive team available and approachable. It makes our frontline team feel safe enough to say they have a big problem and they need some help to solve it."

Asking for Help

Githu, who first participated in the harm collaborative as a unit leader, points out that it is important to give staff members a way to seek help without taking on all responsibility for fixing a problem.

"Too often, you hear about people saying they brought up a concern and then it got assigned to them to fix. But if I knew how to fix it, I wouldn't have asked for help," Githu says. "One thing this collaborative did for me was provide a way to say 'I need help. I can't fix this and I'm bringing it to you to escalate it.'"

Bailey reports to the executive team at subsequent meetings on the progress of action items and process improvements, which she says the executives appreciate.

"What would happen historically is that they would hear about an event one time and never have the opportunity to hear about the resolution, or if there was one. This way, they can be assured that these issues we raise aren't falling off the side of the desk, and we're actually acting on them in meaningful ways," Bailey says.

Githu also asks unit leaders who performed apparent cause analyses to return for updates after their original presentations to the harm collaboratives. They tell the executives about progress with action items, any barriers they encountered, and any new instances of the safety event.

Clarity of Meeting's Purpose

The harm collaborative works only because the executive team attends regularly, Githu says. They attend regularly because they find value in the meetings, she says.

Clarity about the goal of the meeting also is key to making them work, Bailey says. The meeting is not intended as a time to solve the problem.

"We will have good conversations about the potential solutions, but we don't try to solve the problem then and there. We're identifying the issue and deciding where to take the problem to be solved, making sure we're engaging the right teams in it," Bailey says. "It's important not to go too far down the rabbit hole in this meeting, but rather to make a plan for how we will solve the problem after we walk out the door."

It also is important to assign action item owners, Bailey says. Otherwise, the group may hold a robust discussion and enthusiastically endorse action items that are never addressed once everyone leaves the meeting, she says.

"We've gotten more proactive about saying that, for instance, 'The director of surgical services will take this one.' That helps keep it from being overwhelming to Heather and me, so we don't feel like every single problem and event falls on just us to solve," Bailey says. "This has really strengthened my relationship with the executive team and built my confidence up to know that I can go to them as a resource and they are actively engaged and willing to problem-solve with me."

Building that kind of relationship with executives can be difficult if you do not create a purposeful environment in which you meet regularly, Bailey says. Participating in the harm collaborative has improved the risk management program and patient safety at the hospital, she says.

"Prior to the harm collaborative, there would be safety events that prompted multiple emails and communications between this person and that person. Different people would know about parts of the picture, but no one had the whole picture," Bailey says. "Now that we get that core group together weekly, we can inform everyone, clear up any miscommunication, and talk about the event pretty close to when it happened. We eliminate the need for a lot of those side conversations because we know we can discuss on Thursday at the harm collaborative."

Transparency is necessary for a harm collaborative to function effectively, notes **James Bonner**, LMSW, MBA, director of safety and patient experience for Helen DeVos Children's Hospital. That comes from a just culture and must be conveyed from the top down, he says.

"There is some work around high reliability and just culture that has to not only be understood, but accepted and adopted by those wanting to do this work," Bonner says. "It's easy to read about something like this and think it sounds like something you should do, but it requires us as leaders to change and make these principles come alive. The ability to

talk about harm in this way comes from leadership modeling." ■

SOURCES

- **Laura Bailey**, Senior Clinical Risk Manager, Helen DeVos Children's Hospital, Grand Rapids, MI. Phone: (866) 989-7999.
- **James Bonner**, LMSW, MBA, Director of Safety and Patient Experience, Helen DeVos Children's Hospital, Grand Rapids, MI.
- **Heather Githu**, Safety Specialist, Helen DeVos Children's Hospital, Grand Rapids, MI.

Stark Anti-Kickback Law Refined for Clarity

The Department of Health and Human Services (HHS) recently revised federal anti-kickback laws, changes that are seen as primarily good news for risk managers. The revisions clarify issues that were unclear and easing some restrictions that created compliance risks.

The proposed rules would clarify the Anti-Kickback Statute (AKS) and the Stark Law. The changes come in response to hundreds of comments from healthcare leaders about difficulty complying with the rules.

The changes are a significant advantage to doctors, hospitals, and other direct providers of healthcare services to patients, but provide relatively little relief to makers of prescription drugs and suppliers of durable medical equipment, prosthetics, orthotics, and supplies (DMEPOS), says **Thomas N. Bulleit**, JD, partner with Ropes & Gray in Washington, DC.

The ultimate fate for makers of other medical devices, and of drugmakers, is uncertain because the agencies still are considering and soliciting comments for additional safe harbors/exceptions that could be more beneficial to productmakers, Bulleit says. But in the case of non-DMEPOS medical devices, the rules could be more restrictive, he says.

Physicians, Hospitals Win

The winners with the rule changes are physicians, hospitals, and other healthcare providers, Bulleit says. In contrast, several provisions offer increased risk-sharing and outcome-dependent payments among providers.

The revisions propose three levels of protected value-based arrangements, he says. All require a value-based purpose (VBP) of coordinating and managing care, improving quality, reducing costs without hurting quality, or "transitioning" from quantity to quality payments. But the level of documentation needed to demonstrate that purpose and the uses of the payments are lighter as more risk is assumed, Bulleit says.

"When a party to an arrangement assumes full financial risk for the cost of patient care in a target population, essentially anything goes. There are no significant constraints on payments to that person or entity other than that patient and payer preference must be observed when directing referrals," Bulleit says. "For assumption of 'substantial' or 'meaningful' downside financial risk, there are specific amounts of risk that must be assumed. The parties must be able to establish that the payments are primarily in support of a VBP."

The least amount of required risk-taking has the toughest requirements, Bulleit explains. Care coordination agreements (AKS) and value-based arrangements (Stark) both require written agreements spelling out the purpose and methodology, and require maintaining records payment calculations, he says.

The AKS provisions have specific standards, and the remuneration may only be in-kind. There also would be other changes to existing provisions that would reduce restrictions and allow more compensation arrangements to qualify for AKS safe harbors and Stark exceptions, Bulleit says. *(For more on some of the rule changes*

EXECUTIVE SUMMARY

Proposed rule changes regarding anti-kickback restrictions offer compliance relief to physicians and hospitals. The revisions propose three levels of protected value-based arrangements.

- The effect on drugmakers and medical device manufacturers is uncertain.
- Onerous documentation requirements for part-time arrangements would be eased, allowing a larger number of arrangements to qualify.
- The definition of fair market value would no longer be qualified by the requirement that the measurement must be based on an arms-length transaction.

favorable to physicians and hospitals, see the sidebar on page 138.)

The rules include new provisions to address the increasing focus on value-based care, says **Karl Thallner**, JD, partner with Reed Smith in Philadelphia. Hospitals and health systems need to enter arrangements with physicians that include financial incentives to help the network achieve the objectives of improving quality and lowering costs, he notes, so HHS is acknowledging that existing law can stand in the way.

"Providers have been concerned that the Stark Law and the Anti-Kickback Statute create regulatory barriers to building the kind of financial relationships with providers that are necessary to incentivize them to row in the same direction and achieve value," Thallner says. "These proposed regulations create exceptions under those statutes that are aimed at allowing those kinds of arrangements."

Other parts of the revisions are intended to clarify interpretations that are fundamental to compliance, aside from value-based concerns, Thallner notes.

"These rules provide some real relief for the concerns that healthcare organizations have had about how their relationships with physicians could be interpreted to be violations of these laws," Thallner says. "The consequences of the violation are so great that it's been hanging over the heads of many in the healthcare industry for some time now. I think the interpretations are in line with what the industry wanted, what they hoped would be the interpretation in their favor."

Some of the value-based proposals are geared more to specific sectors of the healthcare industry, says **Nicole Aiken-Shaban**, JD, an attorney with Reed Smith in Philadelphia. For instance, certain device manufacturers may be left wondering about the propriety of some products or services they tried to pigeonhole into existing safe harbors, she says.

"Now, the government is saying they're not sure you're contributing directly to patient care the way you need to for these value-based arrangement protections," Aiken-Shaban says. "Those arrangements may be subject to more scrutiny than they originally thought."

Drug and Device Makers Lose

The clear losers are the drug and device makers, Bulleit says. Along with laboratories and suppliers of DMEPOS, drugmakers are expressly excluded from the class of value-based enterprise participants (VBEPs) who may take advantage of the new financial arrangements that would be authorized under the AKS, Bulleit says. Drug and device makers already are essentially unregulated under Stark, he notes.

"Makers of medical devices other than DMEPOS are not expressly excluded, though the commentary indicates that HHS is considering which kinds of device makers that ought to be allowed to participate," he says. "One imagines that makers of physician preference items, like implants, may be least likely to be allowed in, while makers of large capital equipment may make the cut. Drug and device makers might benefit from a revised AKS safe harbor for warranties that would allow warranties on bundles of products. Since this is restricted to products that are reimbursed under the same Medicare payment, this may prove a pretty narrow opening."

HHS is seeking more comments, so drug and device makers may have another bite at the apple, Bulleit says.

Specifics on Rule Changes

Bulleit offers further analysis of the proposed rule changes:

• **Full financial risk.** When a VBE is financially responsible for the cost of all items and services covered by the payer for a target population, essentially anything goes that has a VBP.

VBP means for a target population, the arrangement has the purpose of coordinating and managing care, improving quality of care, appropriately reducing costs (or growth in expenditures) without reducing quality, or "transitioning from healthcare delivery and payment mechanism based on the volume of items and services provided to the mechanism based on the quality of care and control of costs of care." While there are no defined standards, records of methodology for determining payments must be maintained. As a practical matter, it will be necessary to maintain documentation that expresses the VBP.

• **Substantial downside risk (SDR) for AKS and meaningful downside risk (MDR) with Stark.** There are specific standards for the levels of financial risk that must be undertaken. For the AKS safe harbor, to have SDR, the VBE must be at risk for 40% of repayment obligations under a shared savings arrangement, 20% of total loss of a bundled payment arrangement, or a defined subset of total cost for a prospective payment arrangement. The VBEP must be at risk for 8% of the VBE's risk, or must be paid on a fully or partially capitated basis; or, if the

VBEP is a physician, may rely on the Stark standards for MDR.

The value-based arrangement (VBA) must include a VBP. The remuneration must be used primarily to engage in a VBA directly connected to the items and services for which the VBE is at SDR, Bulleit explains. There is no specific writing or recordkeeping requirement, but to establish a VBP and the uses of the remuneration, it will be necessary to create a written plan and method for recording compliance, he says.

Under Stark, to carry MDR, the physician must be at risk to repay the DHS entity with which he or she has a financial relationship 25% of remuneration received, or be responsible prospectively for all or a defined set of covered patient care items and services for each patient (effectively partial capitation). This does require a written description of the downside risk, and maintenance of records of the methodology for determining and payments made for six years, Bulleit says.

• Care Coordination Arrangements (CCA). The least amount of required risk-taking has the toughest requirements. For the AKS CCA safe harbor, only in-kind remuneration is permitted, and it must be used primarily to engage in a VBA that is directly connected to care coordination and management using evidence-based, valid outcome measures.

The recipient must be at risk for 15% of the offeror's cost, Bulleit says. This arrangement must be in writing, defining offeror cost and the percentage of the recipient's contribution, and is subject to monitoring and assessment requirements.

There are no specific financial standards for the Stark VBA exception, but the VBA must be in writing with a description of the methodology, performance standards, and the same record maintenance requirements as the other Stark exceptions, Bulleit says.

The proposed revisions should ease a risk manager's worries over compliance in many situations, although close oversight still will be necessary, Thallner says.

Part-Time Documentation Eased Among Many Favorable Rule Changes

The proposed changes to federal anti-kickback laws contain many favorable features, explains **Thomas N. Bulleit**, JD, partner with Ropes & Gray in Washington, DC. These include:

- The changes would alter the Anti-Kickback Statute so that the onerous requirements for documenting part-time arrangements would be removed from the personal services safe harbor, allowing more arrangements to qualify;
- Outcome-based payments (except from drugmakers, DMEPOS sellers, and laboratories) would be removed from the definition of remuneration, Bulleit notes. A payment would be outcome-based if it resulted from a collaboration to measurably improve quality of care or appropriately and materially reduce costs (or growth of expenditures) while maintaining or improving quality of care;
- Services paid under the Inpatient Prospective Payment System would be removed from the definition of DHS. This would free up hospital relationships with physicians who do not make use of hospital outpatient services, Bulleit says;
- The definition of fair market value would no longer be qualified by the requirement that the measurement be based on an arms-length transaction between parties not otherwise in a position to generate business for each other;
- Productivity bonuses paid to physicians in a group practice could be based not only on personally performed services, but also on "incident to" services performed by nonphysician staff, Bulleit says;
- The definition of when a payment arrangement "takes into account" the volume or value of referrals or other business generated would be narrowed to apply only if the formula includes referrals that result in an effect on the physician's compensation that positively correlates with the physician's referrals (or based on a predetermined correlation), Bulleit explains. This also works in reverse for payments from a physician to a DHS entity. It would no longer be necessary to have Stark concerns with, for example, utilization control measures that reward a reduction in medically unnecessary services, Bulleit says;
- A new exception would allow commercially reasonable payments of up to $3,500 per year (adjusted annually for inflation) from a DHS entity to a physician for FMV items and services provided by the physician, including space and equipment rental, but excluding percent of revenue and per-unit charges "to the extent that such charges reflect services provided to patients referred." ■

"The consequences of violating these laws is so great that healthcare organizations need to exercise a high degree of care and diligence to ensure that arrangements with other referral sources or recipients are proper," Thallner says. "The exceptions that had been in place had been so narrowly drafted that healthcare organizations had no choice but to self-disclose when they realized an arrangement did not meet the exception, but there are new exceptions that are broader and may allow you to conclude the arrangement was compliant. There may be a bit of relief now if potentially noncompliant arrangements had been discovered." ■

SOURCES

- Nicole Aiken-Shaban, JD, Reed Smith, Philadelphia. Phone: (215) 851-8173. Email: naiken-shaban@reedsmith.com.
- Thomas N. Bulleit, JD, Partner, Ropes & Gray, Washington, DC. Phone: (202) 508-4605. Email: tom.bulleit@ropesgray.com.
- Karl Thallner, JD, Partner, Reed Smith, Philadelphia. Phone: (215) 851-8171. Email: kthallner@reedsmith.com.

Avoid the Top Mistakes in Handling Medical Malpractice Claims

A medical malpractice claim is never a walk in the park, but there are ways to make the experience worse and ways to make it better. Becoming aware of some of the most common missteps can help risk managers make the best of a difficult situation.

Poor decisions can change the course of malpractice litigation, says **Roger Harris**, JD, partner with Swift Currie in Atlanta.

"I've had cases that were very defensible on the front end, but then something happens during the course of the litigation that changes the dynamics," Harris says.

One of the biggest mistakes that healthcare organizations make in medical malpractice cases is going back into the medical record to change information, Harris says.

"I don't want clients altering the medical record at any time, but I've been in situations where once the lawsuit was filed and served, someone decides they need to go back and amend the medical record," Harris says. "There are legal ways to amend the medical record, but that does not involve going back once you've seen the claims in the allegation and trying to cover yourself. I've seen that, and it never turns out well."

A good practice is to immediately lock down the chart when a lawsuit is served, Harris says. Any attempt to alter the chart at that point is foolish because, particularly with electronic charts, it is easy to see when a chart was altered, how, and by whom.

"I tell clients that I do not want to see an audit trail that shows them going back into the chart after the lawsuit is filed, even if they don't change anything," Harris says. "Most plaintiffs are not going to continue seeing the physician once a lawsuit is filed, so there is no good reason to enter that chart again."

Risk managers also must be on alert for physicians who want to reach out to patients and talk them out of the lawsuit, Harris says. Communication between the physician and the patient or family can be appropriate and beneficial, including expressions of remorse, but Harris says that does not extend to the physician trying to talk them out of suing. That especially is true once the lawsuit is in motion, he says. Harris tells defendant physicians not to contact a plaintiff once the lawsuit has been filed.

"Once the lawsuit has been filed and served, physicians may want to reach out and try to stop it immediately, but that can become a mistake," Harris says.

Those mistakes may happen infrequently, but the effect on a case can be quite serious, he says. Like much of what risk managers deal with, this can be about stopping something that is both infrequent and potentially costly, Harris says.

EXECUTIVE SUMMARY

Common mistakes can complicate the defense of a medical malpractice case. Some of the mistakes occur before the lawsuit is filed, and some after.

- Take extra care to document adverse events.
- Avoid altering documents in hopes of improving the defense.
- Control how physicians communicate with family and patients regarding a lawsuit.

Some of the most damaging errors can occur after the clinicians know there is a substantial risk of a malpractice lawsuit but before the lawsuit is filed, notes **Carol Michel**, JD, partner with Weinberg Wheeler in Atlanta. There can be situations in which everyone involved knows there is potential for an adverse outcome that could lead to a lawsuit. That should prompt the healthcare professionals to begin managing that potential litigation right away, she says.

Unfortunately, the stress of the moment can make that difficult, she says. Michel recalls a case involving neonatal resuscitation in which the clinicians worked relentlessly to save the child but could not.

"It was understandable that after the resuscitation everyone was tired and wiped out, emotionally drained, but they didn't put the necessary time into documenting what had occurred," Michel says. "The documentation was wildly inaccurate and, as it was documented, suggested that the team had not comported with the standard of care."

That case was saved by the father's videotape of the birth and resuscitation, which captured the team adhering to the standard of care. That was an unusual case in which there happened to be video evidence disproving the clinical team's own documentation suggesting inadequate care, Michel says.

"Absent that video, the team couldn't recall specifically after the fact at what minute they gave another dose of epinephrine or another dose of bicarb. Without that video, we would have been sunk," she says. "Particularly when there has been a significant event, take the time to gather everyone and get the documentation right. Make sure it is thorough and doesn't conflict with other documentation in the record, that it doesn't create a false impression of what occurred."

Michel emphasizes the need for good communication with patients and family members after such an event. Once a lawsuit is filed, direct communication is forbidden. But after a significant event, good communication can help avoid the lawsuit, she says.

"I've had cases where something bad happens and everyone disappears because no one wants to be the one who delivers the negative information to the patient or family. It creates a lot of concern, mistrust, and anxiety on the part of the family and patients," Michel says. "I've had cases where one person was not sued because they were the one that sat down and held hands with the family, cried with the family, and showed compassion. They were the ones who stepped up to the plate and talked to the family when no one else would."

Disorganization is another common error with malpractice litigation management, says **Jeff Kerr**, JD, a former litigator and the CEO of the fact management company CaseFleet in Atlanta. He advises attorneys and serves as an expert witness related to discovery and management of facts in cases, such as how to preserve key information and avoid mistakes that lead to weaker cases or spoliation charges.

"Disorganization sort of feeds all the other problems that can come up along the way, like not knowing what documents are relevant, not knowing what documents to look for and preserve, and failing to understand the timeline," Kerr says. "Even before the lawsuit is filed, an organized record can help you anticipate what kinds of claims might be made or where there might be negligence."

A chronology of events is crucial, Kerr says. "Never underestimate the value of having chronology, right down to the second whenever possible. Knowing the chronology will tell you what documents are important and keep everything tied to the facts of the case," Kerr says. ■

SOURCES

- **Roger Harris**, Partner, Swift Currie, Atlanta. Phone: (404) 888-6175. Email: roger.harris@swiftcurrie.com.
- **Jeff Kerr**, JD, CEO, CaseFleet, Atlanta. Phone: (800) 968-3994.
- **Carol Michel**, JD, Partner, Weinberg Wheeler, Atlanta. Phone: (404) 832-9510. Email: cmichel@wwhgd.com.

Uptick in Investigations Expected for 2020; Data Volume Growing

Healthcare risk managers can expect a greater focus on internal investigations and audits in 2020, with much of it aimed at heading off government inquiries with potentially large consequences.

Healthcare organizations are taking a path similar to many other industries in trying to police themselves before an outside entity intervenes, says **John Kihlberg**, senior director for engagement and client management with H5, a legal technology company in San Francisco.

"We're seeing companies facing a lot more internal investigations, with some of those coming from audit programs and special investigation units focused on trying to prevent some of the regulatory investigations that could be triggered if there is an issue," Kihlberg says. "They are proactively looking at that internally, more than they did before, to try avoid these issues turning into a major problem when regulators get involved."

At the same time, healthcare organizations are conducting more internal investigations regarding compliance, expenses, and mandatory reporting to government agencies, he says. In a recent survey about internal investigations by H5, 20% of respondents in healthcare/life sciences indicated their companies faced more than 100 investigations per year, compared to 22% of respondents overall.

> HEALTHCARE ORGANIZATIONS ARE ADOPTING A HYBRID APPROACH TO DATA COMPLIANCE, USING MORE HUMAN RESOURCES ALONG WITH TECHNOLOGY.

Fifty-seven percent of healthcare/life sciences respondents said their companies proactively monitor electronic data to identify potential wrongdoing, compared to 67% industrywide. Thirty-nine percent of respondents in healthcare/life sciences said that more than half of their investigations involve the preservation and/or collection of employee data. *(The survey report is available online at: https://bit.ly/2PWhr6d.)*

Although investigations are up across all industries, healthcare is faced with increasingly complex compliance requirements for data management, notes **Sheila Mackay**, managing director of eDiscovery Services with H5. For instance, the General Data Protection Regulation law on data protection and privacy for all individual citizens of the European Union addresses the transfer of personal data outside the EU.

Healthcare organizations are adopting a hybrid approach to data compliance, using more human resources along with technology, Mackay says.

"The data are growing so fast, both in volume and variety, that it is sometimes challenging for internal employees to figure out where the sensitive data reside. Healthcare has so much sensitive data. They are hit especially hard by the advent of new technology that may include those data in forms and in locations they haven't seen before," she says. "They have to become faster and more effective at identifying those data, so that is part of what is spurring this uptick in internal investigations." ■

EXECUTIVE SUMMARY

Healthcare organizations are likely to see an increase in internal investigations in the coming year. The primary causes are a growing emphasis on compliance and the advent of new technology creating data risks.

- Slightly fewer healthcare respondents in a survey said they proactively monitor electronic data security, compared to other industries.
- Many healthcare organizations report that more than half of their internal investigations involve the preservation of employee data.
- Companies are using a combination of increased human resources and new technology in response to growing volumes and types of data.

SOURCES

- **John Kihlberg**, Senior Director, Engagement and Client Management, H5, San Francisco. Phone: (866) 999-4215. Email: jkihlberg@h5.com.
- **Sheila Mackay**, Managing Director, eDiscovery Services, H5, San Francisco. Phone: (415) 757-8311. Email: smackay@h5.com.

Larger Claims Increasing, Leading to Higher Premiums

Hospitals may see premium increases and other changes to their medical malpractice insurance coverage because of difficulties facing the insurance industry, including a rise in large claims.

Hospitals will experience an annual loss rate of $2,960 per occupied bed and $5,260 per employed physician for professional liability events in 2020, according to the recent Hospital and Physician Professional Liability report from Aon, a healthcare consulting firm.

Labor and delivery issues are more severe than claims related to other allegations, with an average total cost of more than $450,000, the report says. The average severity for children's hospitals is growing at higher rates than other hospitals, the data indicate.

"While self-insured layers continue to see modest annual trends, the frequency and average severity of losses greater than $5 million continues to increase. After an increasing number of large medical malpractice verdicts following years of premium decreases, all stakeholders in malpractice liability are under pressure," the report says. "These pressures include premium rate increases, self-insured retention increases, and insurance carrier capacity reductions." *(The report is available for purchase online at: https://aon.io/2rj3btT.)*

Self-Insured Claims Steady

Claims with payouts of up to $2 million, representing mostly the self-insured claims, have been holding steady, says **Virginia Jones**, FCAS, MAAA, an actuary for Aon in Chicago and lead author of the study. But claims of greater than $5 million are increasing, she says.

"Not only are we seeing more, but the average cost of a claim greater than $5 million is higher than it was five or six years ago," Jones says. "That's one part of what is making this a challenging market for medical malpractice and possibly driving some of the premium increases that are surprising people when they see their smaller claims holding steady."

Hospitals are feeling additional pressure from carriers for risk reduction and data collection, and some insurers are limiting their coverage in certain markets, Jones notes.

"It's important for the hospital risk managers to start thinking about what they can do to offset some of these changes imposed by the insurers, which are almost inevitable," she says. "This will make risk managers even more important than ever, but they also have to get more creative and think outside the box to find solutions."

'It Takes a Village'

Insurance policy review will be vital to getting the most coverage at the lowest cost, Jones says. Risk managers should look at issues such as batch coverage language, making sure it is appropriate for the hospital or health system. It also is important to cultivate good relationships with insurers, brokers, and actuarial consultants, Jones says.

"It takes a village to approach the market today. You want to create a cohesive team among all these players that a risk manager has to engage in the insurance process," Jones says. "It also is important for risk managers to understand what is happening in the market so that they can communicate that up the line in their own organization, and so that they can respond most effectively to those market changes. The insurance coverage they have should work for their organization, their risk appetite, and that will require a cohesive approach that gets everyone on the same page to find the right solution." ■

SOURCE

- Virginia Jones, Actuary, Aon, Chicago. Phone: (312) 381-1000.

EXECUTIVE SUMMARY

The medical malpractice insurance market is hardening in response to an increase in claims with large payouts. Hospitals and health systems may feel the effects even if their own claims are stable.

- Hospitals will experience an annual loss rate of $2,960 per occupied bed in 2020.
- Claims with payouts of up to $2 million, representing mostly the self-insured claims, have been holding steady.
- Claims of greater than $5 million are increasing.

Government Moving to More Risk Arrangements Based on Quality

The Center for Medicare & Medicaid Innovation (CMMI) wants 100% of providers in upside/downside by 2025 and is using the Bundled Payments for Care Improvement Advanced (BPCI Advanced) model, primary care models, and (increasingly) more mandatory models to get there.

This pressure from the government will put quality directors in a position to highlight their work and play an important role in the organization's future financial success, says **Dave Terry**, CEO and co-founder of Archway Health, a company in Watertown, MA, that helps hospitals with bundled payments.

"[CMMI] said last winter that their goal is to move 100% of Medicare providers into some type of meaningful up and downside risk arrangement, which is a pretty big deal. Previously, under the Obama administration, they were looking for value-based contracts, but those could be upside or downside. A lot of providers chose just upside only," Terry explains. "The current team is focused on moving providers to real risk arrangements because you only see improvements in performance, quality, and costs when there is a downside component to the contracts."

BPCI Advanced is a model that covers services within a 90-day clinical episode, with a clinical episode defined as beginning with an inpatient admission for an inpatient procedure or the start of the outpatient procedure. Such an episode continues for 90 days after discharge or the procedure. Good performance on quality measures and costs results in more revenue — the upside — but money can be lost if goals are not met — the downside.

BPCI Advanced qualifies as an Advanced Alternative Payment Model under the Quality Payment Program created by the Medicare Access and CHIP Reauthorization Act. Healthcare providers can choose to participate in up to 29 inpatient clinical episodes and three outpatient clinical episodes.[1]

All alternative payment models include a quality improvement component. Quality professionals will become increasingly important as their organizations explore the options and move forward, Terry says. No matter what model is used, quality metrics will be crucial to seeking the upside rewards of the model. "If the provider organization isn't able to demonstrate with real data that they are improving on quality, the reimbursement will be impacted," Terry says. "I think that's a pretty big deal for quality professionals." ■

REFERENCE

- Centers for Medicare & Medicaid Services. BPCI Advanced. Available at: http://bit.ly/2lDIPsp. Accessed Nov. 12, 2019.

California Law Could Cost Hospitals Millions

Healthcare organizations across the country should be keeping an eye on the California Consumer Privacy Act (CCPA), which will go into effect Jan. 1, 2020. Failure to comply with this new rule can result in significant penalties, and it is a mistake to think HIPAA compliance will protect organizations.

Some healthcare companies are incorrectly assuming they are exempt from CCPA compliance because of superseding HIPAA guidelines, says **Ryan P. Blaney**, JD, partner with Proskauer in Washington, DC.

As providers expand beyond traditional care delivery to focus on digital innovation and, in some cases, venture capital, parts of an organization still could be subject to CCPA and other emerging state-based legislation requirements, Blaney explains. Not knowing one's exposure could end up costing healthcare organizations millions, he says.

Healthcare organizations based outside California could be subject to the privacy requirements of CCPA if they are doing business in the state, which can be construed broadly, Blaney explains. Compliance with HIPAA does not necessarily mean the organization will be in compliance with CCPA, he says.

"Although there is an exception under CCPA for healthcare companies that fit some criteria, not all healthcare companies will fit within that exception. It is important not to assume that just because you deal in healthcare information, you are going to fall under the healthcare exception to the CCPA," Blaney says. "There is an analysis that needs to be done to be sure you fall squarely within that exception." ■

HEALTHCARE RISK MANAGEMENT™

CE INSTRUCTIONS

To earn credit for this activity, please follow these instructions:

1. Read and study the activity, using the provided references for further research.
2. Log onto **ReliasMedia.com** and click on My Account. First-time users must register on the site. Tests are taken after each issue.
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 test, your browser will be automatically directed to the activity evaluation form, which you will submit online.
5. Once the completed evaluation is received, a credit letter will be emailed to you.

CE QUESTIONS

1. **How often does the harm collaborative at Helen DeVos Children's Hospital meet?**

   a. Twice a year
   b. Monthly
   c. Weekly
   d. Daily

2. **What is the purpose of the harm collaborative meeting?**

   a. Solve the problem.
   b. Identify a safety or process issue and possible solutions.
   c. Determine noncompliance with regulations and laws.
   d. Assess the potential liability for safety events.

3. **How many levels of protected value-based arrangements are in the proposed changes to the Anti-Kickback Statute and Stark Law?**

   a. One
   b. Three
   c. Five
   d. Seven

4. **Hospitals will experience an annual loss rate of how much per occupied bed in 2020, according to the recent Hospital and Physician Professional Liability report from Aon?**

   a. $2,960
   b. $1,960
   c. $5,960
   d. $7,960

CE OBJECTIVES

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

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

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

Incorrect Diagnosis Leads to Patient Refusing Cesarean Section, Infant's Permanent Injuries

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

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

***Elena N. Sandell**, JD*
UCLA School of Law, 2018

News: A pregnant teenage patient chose to proceed with a vaginal delivery, but the patient's child suffered permanent injuries. The patient was admitted to the hospital experiencing pre-eclampsia, and the patient alleged that her care providers gave inaccurate and incorrect predictions about the risks of giving birth. Because of the providers' advice, the patient gave birth vaginally rather than by cesarean section. The patient's child was born without a pulse, required resuscitation, and suffers from severe cerebral palsy.

The patient filed suit on behalf of her child against the hospital, alleging that the incorrect diagnosis and advice constituted medical malpractice. The hospital denied any wrongdoing. A jury awarded $229 million, which was subsequently reduced to $205 million due to a state statutory maximum.

Background: In 2014, a 15-year-old patient was pregnant with her first child. At 25 weeks' gestation, the patient was admitted to the labor and delivery unit of a local hospital in pre-eclamptic condition. Following her admission, the hospital began monitoring the fetal heart rate and the mother's high-risk condition. Around 7:30 p.m. on the day of admission, the care providers at the local hospital decided to transfer the patient via helicopter to a higher acuity medical center based on the patient's severe pre-eclamptic condition. At this hospital, the patient's condition was monitored throughout the night. An ultrasound revealed an estimated fetal weight of 664 grams.

BECAUSE OF THE TRAUMATIC BIRTH, THE CHILD SUFFERS FROM SEVERE DEVELOPMENTAL DELAYS, CEREBRAL PALSY, CANNOT WALK, AND WILL REQUIRE CONSTANT MEDICAL CARE.

The next morning, the NICU team discussed the plan of care with the patient and erroneously stated that the perceived lack of fetal growth indicated that potential outcomes for the baby were very poor, specifically indicating a high probability of neurological and physical defects and no chance of the baby's brain being normal. A neonatologist also was consulted and reported that the baby would be born sick with high likelihood of death or neurodevelopmental disability. As fetal monitoring continued, physicians presented increasingly dire scenarios for the baby's survival. Physicians informed the patient that her child's development was significantly less than originally expected, based on a new approximated weight of 400 grams instead of 660 grams as initially estimated. At 11:30 p.m., fetal monitoring was discontinued.

Two days after the patient's transfer, care providers decided to induce labor, although the patient allegedly understood that the chances of the baby's survival delivered at this stage and through vaginal delivery were poor. The patient indicated she did not wish to undergo a cesarean section, and fetal monitoring was discontinued.

The patient received five doses of misoprostol for induction of labor. The patient progressed to complete dilation; however, when the obstetrics and NICU teams were called to the room, the infant's head was crowning and partially out. The infant's weight at birth was 670 grams. She was immediately transferred to the NICU, intubated, and resuscitated since she was not breathing and did not present a heart rate.

Because of the traumatic birth, the child suffers from severe developmental delays, cerebral palsy, cannot walk, and will require constant medical care. The patient sued the hospital on behalf of her child, claiming lack of informed consent and negligence resulting in her child suffering such injuries. The hospital denied wrongdoing and liability.

After a trial, a jury awarded $229 million, consisting of $3.62 million for past medical expenses, $1.02 million for lost earnings, $25 million for noneconomic damages, and $200 million for future medical expenses and damages. The judge subsequently reduced the verdict to $205 million based on a state statutory maximum for medical malpractice actions.

What this means to you: This case reveals how a patient's circumstances can dramatically affect the size of a verdict, regardless of the underlying type of malpractice. Failures to diagnose or incorrect diagnoses are common types of malpractice when a reasonable physician in the same or similar circumstance would have accurately diagnosed the patient. But not all misdiagnoses result in the same amount of injury, and this is directly correlated to the amount of a resulting verdict in the case of liability. In this case, the injured party is perhaps the most vulnerable — a newborn child — and the injuries were so substantial as to require lifetime care. Accordingly, these circumstances supported a jury award of more than $200 million, with the majority for future expenses. While physicians and care providers should exercise caution and provide diligent and thorough care for all patients, additional caution may be exercised for patients who are more likely to suffer life-threatening or substantial injuries.

The substantial award in this case indicates that the jury aimed to ensure that the young mother and her child would have the necessary means to cover the significant and inevitable medical expenses incurred throughout the child's life. As indicated in the complaint, if the physicians had adequately informed the patient about the risks and alternatives for delivery, the child could have been born without complication. However, the child suffered significant injuries because the physician provided incorrect information about the weight of the fetus and providing incomplete information about her delivery options and the related risks. Unfortunately, the physicians in this case were incorrect about the fetal weight: at 660 grams, pursuant to the initial estimate, the fetus was a normal weight for the gestational age of 25 weeks.

Under these circumstances, the mother's pre-eclampsia was more medically urgent and a more significant problem, yet pre-eclampsia can be safely and effectively managed with physician supervision. The information, or lack thereof, presented by the physicians led the patient to discontinue fetal monitoring and proceed with induced labor when, in fact, the pregnancy could have continued to term once the mother's pre-eclampsia was brought under control. The patient claimed that it was unclear that inducing labor at such an early gestational age posed tremendous risks to her child. She further alleged that had the implications of her choices been fully explained, she would have chosen to continue monitoring the fetus and considered other options.

Another important lesson from this case is the necessity and importance of expert witnesses. In this case, the plaintiff retained an expert witness to offer opinions on the applicable standards of care. The plaintiff's expert witness comprehensively outlined multiple deviations from the standards of care committed by the defendants and opined that had the standard of care been followed, the child would have been born without the injuries. In other words, the expert opined that the injuries suffered by the infant were directly and proximately caused by the negligence of the defendants.

According to the expert's analysis, the physicians acted negligently from the moment of the plaintiff's transfer to the hospital. First, based on ultrasounds and estimated fetal growth, the patient's fetus was consistent with normal fetal development; thus, the physicians should have advised the patient that her fetus was viable. When a second estimate of fetal weight was found to differ from the original weight, all care providers involved should have turned their attention to determining which weight was correct. This would require multiple evaluations by multiple practitioners until a consistent result was obtained and determined to be correct by all involved. This applies to any test result or data measurement involved in determining critical steps in patient care.

In this case, the care providers incorrectly assumed that the new weight was correct and disregarded the original reading. By informing the patient that her fetus was underdeveloped and would not

have a good chance of survival, the physicians deviated from the standard of care. Based on a subsequent and more comprehensive ultrasound, the physicians estimated the fetus' weight to be 250 grams less than the actual weight. This mistake led to an erroneous and increasingly negative prognosis, which convinced the patient to choose not to undergo a cesarean section. Furthermore, fetal monitoring should not have been discontinued under these inconsistent and dangerous circumstances, and the care providers should have advised the patient that a cesarean section would reduce the risks to the child. Finally, the physicians either erroneously performed or misread ultrasounds and inaccurately concluded that the fetus exhibited signs of severe intrauterine growth restrictions.

According to the plaintiff's expert, absent negligence, the patient would have been advised to undergo delivery through a cesarean section, which was the best option to maximize the well-being of both the patient and her child. Unfortunately, as a direct result of the physicians' actions, the patient believed that her fetus had a near-zero chance of survival; the patient held out hope based on her request for resuscitation. If she had been presented accurate information and options, she would have elected to undergo a cesarean section. The physicians in this case did not enable the patient to make that decision, and their multiple deficiencies constituted actions below the applicable standard of care, resulting in their liability and the substantial verdict. ■

REFERENCE

Decided on July 1, 2019, in the Circuit Court for Baltimore City, Case Number 24C18002909.

Court of Appeals Holds That Failure to Diagnose Defects in Fetus Did Not Cause Mother's Death

News: A woman underwent a third trimester abortion and subsequently suffered complications. She developed an amniotic fluid embolus and died. The woman's husband filed a medical malpractice and wrongful death suit against the physician who examined the patient and allegedly failed to identify abnormalities in the fetus earlier during the pregnancy. During the litigation, the plaintiff amended his complaint to include a theory of liability based on negligence. The defendant physician brought a motion for summary judgment. The trial court found that the physician established that any alleged departures from the applicable standard of care were not the proximate cause of the patient's injuries.

The plaintiff appealed the ruling granting the physician's motion, but the appellate court upheld the ruling. The appellate court confirmed that the plaintiff failed to demonstrate that a triable issue of material fact existed, and that judgment for the physician was proper.

Background: In October 2012, a woman 20 weeks pregnant underwent a sonogram of her fetus. A maternal fetal medicine physician performed and analyzed the scan. Although the physician noted some asymmetry, he determined that the study was normal and recommended a repeat scan in six to eight weeks. At the end of January 2013, a second ultrasound was performed. The physician who interpreted the second scan noticed abnormalities in the fetus' cerebral development. In particular, the physician noted that the fetus' cerebral ventricles appeared to be dilated and recommended further evaluation and studies. A third ultrasound conducted three days later revealed bilateral moderate ventriculomegaly.

Following the third ultrasound, the physician ordered further testing and referred the patient for a fetal MRI. The MRI revealed agenesis of the corpus callosum and polymicrogyria, a condition characterized by abnormal development of the brain, which can lead to severe intellectual disability, problems with movement, and seizures that are difficult or impossible to control with medication. The MRI results worsened the initial findings from the ultrasounds and confirmed that the fetus suffered from developmental abnormalities. After receiving counseling, the patient opted to terminate the pregnancy. The patient was in her third trimester, and the termination procedure presented higher risk compared to first or second trimester abortions. Nevertheless, the patient underwent the abortion, which was performed over the course of four days in early February 2013. On the fourth day, the patient was discharged.

However, shortly after arriving home, the patient's condition rapidly deteriorated, and she returned to the hospital the next morning, where she subsequently passed away. The medical examiner ruled the cause of death to be disseminated intravascular coagulation due to an amniotic fluid embolus.

A year after the patient's death, the patient's husband filed a medical malpractice and wrongful death suit against the physician who failed to identify the fetal abnormalities at the 20-week ultrasound. The physician denied wrongdoing.

In his defense, the physician submitted an affidavit of an expert in maternal fetal medicine who opined that, because there is no medical basis indicating that a third trimester termination procedure causes an amniotic fluid embolus, the physician's alleged failure to diagnose fetal abnormalities did not cause the patient to sustain, or increase her risk of sustaining, an embolus. After the defendant physician raised this defense, the plaintiff amended his complaint, alleging that the defendant's negligence caused the patient to develop an infection and die of septic shock.

The defendant physician filed a motion for summary judgment, and the trial court found that the physician established that any alleged departures from the applicable standard of care were not the proximate cause of the patient's injuries. The trial court granted the motion and ruled in favor of the physician.

The plaintiff appealed the ruling, but the appellate court confirmed that the plaintiff failed to demonstrate that a triable issue of material fact existed, and that judgment for the physician was proper.

What this means to you: In this case, the alleged wrongdoing focused on the initial ultrasound, with the patient's husband claiming that the defendant physician failed to timely diagnose the patient. The plaintiff claimed that defendant physician's failure to identify abnormalities in the fetal scan performed at 20 weeks was the proximate cause of his wife's death because of amniotic fluid embolus. Under this theory, if the defendant identified such abnormalities in the fetus' brain development, the patient would have chosen to terminate the pregnancy at 20 weeks instead of during the third trimester. It is known that abortions performed during the third trimester present a higher risk of complications compared to abortions performed during earlier stages. Thus, according to the allegations, the riskier procedure caused the patient to develop the embolus that eventually led to her death.

However, according to the defendant's expert, there was no medical evidence to suggest a connection between third trimester abortion and the development of amniotic fluid embolus. This effectively exonerated the defendant of liability because of the lack of causation, which is a necessary element in medical malpractice actions.

Indeed, no evidence was proffered to support the theory that the defendant's lack of an early diagnosis was the proximate cause of the patient's death. Thus, while third trimester abortions do present a higher level of risk, the plaintiff failed to present supporting evidence demonstrating that one of the consequences was the development of amniotic fluid embolus.

As noted by the court, once the defendant moved for summary judgment and satisfied his prima facie burden of presenting evidence indicating that he did not deviate from the standard of care, the burden of proof shifted onto the plaintiff. Rather than providing evidence in support of his claim, the plaintiff sought to amend his complaint and introduce a new theory of causation: The patient died due to negligence of the defendant, which had caused an infection resulting in septic shock and death.

The appellate court agreed with the defendant that under the circumstances, leave to amend the complaint should not have been granted. The court noted that the action had been filed more than three years prior to the motion to amend the complaint and that the plaintiff aimed at introducing a new theory of liability without giving the defendant notice. Furthermore, the defendant satisfied his burden of proof, and the plaintiff failed to present supporting evidence. Thus, there was sufficient ground to grant a summary judgment in favor of the defendant.

While the plaintiff attempted to amend the complaint to allege an alternative theory of causation to survive summary judgment, those efforts were unsuccessful. Fortunately for the defendant physician in this case, the medical examiner's report identified the cause of death as disseminated intravascular coagulation due to amniotic fluid embolus. Even if the plaintiff had included these alternative allegations in the initial complaint, it is unlikely to have been effective. Plaintiffs are permitted to initially plead contradictory or inconsistent facts, but they cannot be maintained all the way through a trial. If a plaintiff makes factual allegations that conflict with other allegations or are unsupported by the evidence, a defendant care provider should promptly challenge such allegations with evidence — such as the report in this case, or with qualified expert testimony — to dispose of the irrelevant allegations. In this case, the defendant physician successfully dismantled the plaintiff's multiple theories of causation, which defeated the medical malpractice claim. ■

REFERENCE

Decided on Aug. 21, 2019, in the Second Department of the New York Supreme Court, Appellate Division, Case Number 175 A.D.3d 614.

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Avoid Most Common HIPAA Violations With Best Practices, Education

HIPAA breaches can happen even to the best prepared healthcare organizations, but knowing the most common failings can improve your chances of staying in the good graces of the Office for Civil Rights (OCR).

Organizations sometimes have a false sense of preparedness because they put policies in place and think that is enough, says **Lucie F. Huger**, JD, an officer, attorney, and member of the healthcare practice group at Greensfelder, Hemker & Gale in St. Louis. "I see a lot of technical compliance, but one thing I see organizations overlooking on a routine basis is the human element involved," Huger says. "Through those mistakes, even with the best policies in place, you can still be violating HIPAA. People get curious and click on links in phishing emails, which can be very dangerous to an organization. Or, I see it when people work too quickly and provide information about a patient to the wrong person."

Data management and restricted access can address some of the inevitable human failings that lead to HIPAA breaches, says **Jorge Rey**, CISA, CISM, risk advisory services principal at Kaufman Rossin in Boca Raton, FL, which provides business consulting and compliance services. If employees have limited or no access to protected health information (PHI), they cannot release it even accidentally, he explains. "We've seen a lot of healthcare institutions trying to limit the access that everyone has," he says. "They are becoming better at understanding where that data resides to prevent that unauthorized access. Laptops were a big issue for a couple years because data was not encrypted and data were being lost, but we've seen in the past couple of years that is becoming less common."

When training staff and physicians on HIPAA compliance, healthcare organizations should tailor the content to explain what HIPAA compliance looks like in the day-to-day work environment for that organization, says **Melissa Soliz**, JD, an attorney with Coppersmith Brockelman in Phoenix. Leaders should provide practical guidance on how to protect the privacy and security of health information, she says. "HIPAA trainers and educators often forget to cover some of the most basic HIPAA compliance measures that are most effective in protecting the privacy and security of health information," Soliz says.

She cites these examples of important points often overlooked:

- Reminding workforce members to not take any health information outside the organization unless it is necessary to do so and permitted by the organization's policies and procedures;
- Prohibiting workforce members from accessing health information systems through devices such as cellphones or tablets or storing health information on such devices that do not meet HIPAA standards or are not approved for use by the organization;
- Prohibiting workforce members from posting details about or pictures of patients in the workforce members' social media posts;
- Reminding workforce members that paper records containing health information cannot be disposed of in open garbage or recycling bins;
- Instructing workforce members on how to avoid cyberattacks, such as phishing emails;
- Informing workforce members of who to contact if they want to ask HIPAA-related questions, who to contact if they suspect there has been an unauthorized use or disclosure of health information, and where the organization's HIPAA policies and procedures are located.

It is important that the organization maintains robust privacy and security policies and procedures, Soliz says. Further, the organization should implement those policies and procedures through regular training, auditing, and enforcement. The most common mistakes employees make is individual carelessness, such as leaving paper patient records in an unlocked car, clicking on phishing links in emails, or inadvertently disclosing patient health information in a social media post about their

workday, Soliz says. "Educational efforts often focus on abstract privacy and security concepts without providing workforce members with sufficient context to understand how they can be HIPAA compliant within their work environment," Soliz says. "Providing workforce members with concrete examples of what HIPAA compliance and noncompliance looks like will enable organizations to avoid the most common errors."

Soliz cites a recent example in which a small dental practice paid OCR $10,000 as part of a corrective action plan arising out of the practice's response to a patient's social media review, in which the practice disclosed the patient's last name and details of the patient's health condition. *(Read more about this case at: http://bit.ly/2pPYg30.)* "OCR imposed a $2.15 million civil monetary penalty on a health system that lost paper records on over 1,400 patients, allowed a reporter to share a photograph of an operating room containing patient health information on social media, and had an employee who had been inappropriately accessing and selling patient records since 2011," Soliz says of another case. *(Read more about this case online at: http://bit.ly/2Pii0qI.)*

Training should be aligned with the organization's policies and procedures and it must be practical, says **Erin S. Whaley**, JD, partner with Troutman Sanders in Richmond, VA. Too often, organizations provide generic HIPAA training, she says. "The generic trainings are, at best, not based on the organization's policies and procedures and, at worst, inconsistent with the organization's policies and procedures. Customizing generic trainings will help ensure consistency and alignment with the organization's policies and procedures," she says. "Another pitfall is training on concepts instead of practical application of those concepts. By offering real-life examples and horror stories, organizations can help their staff and physicians recognize and avoid risky or noncompliant behavior."

One of the most frequent system-level oversights is failure to perform a complete annual risk assessment, Whaley says. Considering the number of cloud-based solutions, some organizations believe they can rely on their vendors to perform these assessments. However, these organizations are obligated to conduct a thorough assessment for all their systems, she explains. "These assessments may be informed by information from vendors but should not be delegated to the vendors," Whaley says.

In terms of individuals, the most prevalent mistakes usually are simple human error, such as losing a laptop, sending an email to the wrong person, or discarding PHI in the wrong bin, Whaley says. "There is still a surprising amount of paper PHI in practices. Paper PHI must be properly disposed of to ensure destruction," Whaley says. "Organizations should have a secure bin for discarded paper PHI, but the organization may only have a few of these secured bins throughout the facility. For efficiency, individuals sometimes keep a shred box at their desks so that they don't have to walk to the secure bin each time they need to discard a document, even though this may not be consistent with the organization's policies and procedures."

The individual may empty this "shred box" only occasionally when it is full, Whaley explains. If the cleaning crew inadvertently throws this box away in the trash or recycling instead of the secure bin, this could be a breach. Investigating and reporting this type of incident is difficult and completely avoidable, Whaley adds. When providing HIPAA education, it is important to ensure the workforce appreciates that management has bought in relative to compliance, says **Brad Rostolsky**, JD, an associate with Reed Smith in Philadelphia. Training should not be viewed as "something you just need to do," he says. "Beyond that, it's important to do more than provide a HIPAA 101 training," he advises. "Training should spend some time focusing on the actual policies and procedures of the business."

From a system perspective, one of the more common challenges is logistics, Rostolsky says. The bigger the entity, the more challenging it is to communicate information throughout that entity in a timely and efficient manner, he says. "It's important to ensure that a process is in place for the workforce to understand who in the privacy office needs to know what information and when they need to know it," he says. "A basic example of this would be to prospectively designate a particular individual to receive subpoenas, or even just requests for PHI, so that the requests are processed appropriately."

Individuals, on the other hand, often violate HIPAA merely because they do not fully appreciate that one person's action, or failure to adhere to what may seem like an annoying rule, can significantly affect a large business, Rostolsky says.

"To this end, part of training should include examples of where big dollar enforcement actions were triggered by the noncompliant actions of a single individual," he suggests.

Training also should be provided in different forms, says **Michele P. Madison**, JD, partner with Morris Manning & Martin in Atlanta. For example, there should be training at orientation, staff meeting reminders about HIPAA safeguards, and education about ransomware attacks. Healthcare organizations also can conduct phishing exercises to test employee response, sharing the results on an annual basis during the staff member's performance review, Madison suggests.

"One common mistake is providing an initial education forum at orientation and requiring annual review of an

online training program that fails to address the specific job functions or roles of the individual," she says. "The lack of specific and continuous training may not adequately prepare the staff member for his or her job and lead to a mistake that causes a breach."

Another common mistake is failing to provide continuous security awareness training, she says. Such training is a requirement of HIPAA, Madison notes, and technology is constantly changing. Therefore, the organization's security safeguards should be reviewed on a regular basis. Staff should be trained on the new and upgraded security safeguards as well as the vulnerabilities and risks associated with electronically accessing, storing, or transmitting PHI, she says. "[OCR] fines and penalties have focused upon organizations failing to implement a comprehensive security risk analysis. Failing to fully evaluate all mobile devices and the different access points to the organization's information technology infrastructure is a significant risk to the organization," Madison explains. "In addition, when the technology infrastructure changes, even to troubleshoot an issue, the risk assessment should be performed to identify any safeguards that need to be implemented as part of the change to the system."

Social media continues to pose a significant risk for HIPAA violations, says **Susan Tellem**, RN, BSN, APR, a partner with Tellem Grody Public Relations in Los Angeles, which assists providers with their responses to HIPAA violations. Instagram and Facebook create an easy medium for people to violate HIPAA, Tellem says. But beyond those channels, there are many ways healthcare employee can inadvertently disclose PHI and never even realize it, she adds.

"Faxing of some PHI is allowed, but a fax can wind up easily in the wrong hands," she says. "What if a healthcare professional is taking a break and decides to share a photo of what she is eating with an open patient file in the background? Photo sharing among doctors and patients is becoming more common and may be shared by accident." ■

Enforcement Action Follows Predictable Path, Starts With a Letter

A healthcare organization's involvement with OCR may begin with a simple letter acknowledging a complaint and providing guidance documentation related to it, notes **Elizabeth Litten**, JD, partner and HIPAA privacy and security officer with Fox Rothschild in Princeton, NJ. "Sometimes, [OCR] will send a complaint warning letter, knowing that it may be a one-off, but they want to make the covered entity aware and ensure it is complying with HIPAA," Litten explains. "Sometimes, they'll ask the covered entity to respond in some way, but, frequently, if they think it just involves one incident or individual, they will say they consider it closed but will be concerned if the problem persists."

For a more serious concern, OCR will assign a case number and ask for substantial information, such as policies and staff education records. Typically, OCR gives a 30-day deadline, but often will grant an extension if requested. "They may ask for documentation on what occurred, your policies and procedures, how you addressed the incident. They'll ask for very specific information, even financial information, to get a sense of who your business associates are," she says. "They may ask for specific names and titles of individuals involved."

The letter usually says that if an organization does not respond, that will be considered a violation of HIPAA. The course of OCR's response will be determined largely by the nature of the complaint, says **Emily Quan**, JD, an attorney with Weinberg Wheeler Hudgins Gunn & Dial in Atlanta. Impermissible use and disclosure is the most common type of complaint.

"With that complaint, typically, the covered entity will be asked for some information to review the complaint," Quan says. "[OCR is] looking at when this potential violation occurred, whether the entity is covered by the privacy rule, whether the complaint was filed within the usual six months, and whether the incident actually violates the privacy rule." The outcome can be tough to predict. OCR could determine there was no violation, or the agency could rule there was a violation, and levy various civil penalties. Quan says this is why it is vital to conduct a comprehensive risk analysis early. "This is a process that tends to snowball, particularly if this involves a massive health system or institution. There can be a number of offshoots from the investigation, with each one of them requiring time and resources to investigate."

There are countless HIPAA violations every year that are never detected or reported, says **Eric D. Fader**, JD, an attorney with Rivkin Radler in New York City. A media report may trigger an investigation, as with a recent case in which OCR fined a health system more than $2 million after reporters shared a photograph of an operating room screen that included a patient's medical information *(See previous article in this issue for more information.)*

"Sometimes, the OCR will begin an investigation after receipt of a complaint from a patient or other party," Fader says.

"However, I think most often, the filing of a covered entity's or business associate's own breach report with OCR will trigger the investigation."

OCR uses wide latitude when determining potential penalties. Generally, a breach or other HIPAA violation in and of itself will not result in an expensive fine. If the breach affects few people and was identified and corrected promptly, an investigation is less likely. Still, OCR has made a point of publicizing some tiny breaches, just to show that "size isn't everything," Fader cautions.

OCR usually has much less patience and understanding when the covered entity or business associate has not adopted required HIPAA policies and procedures, has not properly trained and retrained its employees (no less often than once per year), failed to conduct required periodic enterprise-wide risk assessments, or failed to investigate and report a breach timely.

The absence of a business associate agreement between a covered entity and its business associate or between the business associate and its subcontractor can compound the potential penalty. "Breaches happen," Fader says. "An entity that has taken HIPAA seriously and that investigates and takes corrective action promptly, and that doesn't attempt to deceive OCR or minimize the severity of its actions, has a good chance of getting off lightly."

Enforcement is not limited solely to the imposition of monetary fines, notes **Matthew R. Fisher**, JD, partner with Mirick O'Connell in Worcester, MA. Enforcement can include investigations, audits, requirements for corrective actions, and private lawsuits, although litigation will not fall directly under HIPAA.

It is difficult to find any pattern for when a fine will be imposed. If there is a particularly egregious violation or the organization can pay a substantial fine, then infractions may be more likely to result in a monetary penalty. "Additionally, OCR is increasingly focused on denial of access problems, which suggests more fines could be coming on that front," Fisher suggests.

An investigation may not necessarily make headlines, but it does affect an organization and take time and resources. For enforcement, OCR's primary options are monetary penalties and/or corrective actions. "Monetary penalties are imposed in few instances, but there does not seem to be any rhyme or reason as to when a penalty will be imposed. Corrective actions often consist of technical advice to help organizations better comply with HIPAA requirements," Fisher says. "Corrective actions will result quite frequently when an interaction occurs between an organization and OCR because some issue of noncompliance will likely arise. A corrective action is often collaborative and not punitive, as OCR wants to see good practices put into place."

Enforcement will follow a standard course of investigation, audit, discussion, determination of baseline issues, and then outcome. The first few stages will consist of document requests and a written or verbal back and forth. Often, the goal is to establish that efforts are in place for an organization trying its best. "Even with the best of efforts, mistakes or issues can arise. The good faith effort at demonstrating compliance will be a big factor in influencing the outcome of an investigation or potential issue," Fisher says. "If an organization is ignoring or deliberately not implementing a policy or procedure required by HIPAA, then issues will arise."

In an ordinary course, the timeframe for resolution of an issue will be a few months. OCR usually will send a document request within one month of a large breach report or an individual complaint filing. From there, an organization will have about two weeks to submit a response. Some time later, OCR will reveal the resolution to the organization. "That is the ordinary course. However, recent monetary penalties seem to take years from the underlying incident," Fisher observes. "There is no indication as to why so much time passes, though it could be that there is a lot of back and forth going on in the background."

The biggest impact on a potential outcome is transparency and taking good faith steps to comply with HIPAA. OCR recognizes that no organization can be perfect all the time. Still, so long as honest efforts are taken, OCR will be willing to work collaboratively.

Sometimes, the OCR investigation reveals relatively minor violations that can be corrected without significant penalties, says **Kimberly J. Gold**, JD, partner with Reed Smith in New York City. OCR may only seek corrective action in these instances. They may seek changes to an organization's HIPAA policies, procedures, and training. In more serious cases, OCR will pursue penalties in addition to corrective action. Criminal charges are seen less frequently. The course of enforcement typically is determined by how egregious a HIPAA violation is in the mind of OCR. "A data breach involving hundreds of thousands of individuals and underlying HIPAA violations, like the failure to conduct a security risk assessment, could trigger significant penalties," Gold warns. "Even the failure to execute business associate agreements has led to penalties. Less serious violations that can be quickly remedied are often easier to resolve without financial penalty."

In addition to cooperating, maintaining strong records (including documentation of policies, procedures, training, and risk assessments) will go a long way with OCR. "Should OCR investigate a large data breach and find no evidence of a risk assessment having been performed, or of any commitment to a HIPAA compliance program, enforcement will be more likely," she cautions. ■