HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE SINCE 1979

INSIDE

Relias Media
From Relias

NOVEMBER 2020 Vol. 42, No. 11; p. 121-132

$50 Million Stark Settlement Shows Risk of Violation, Whistleblowers

The recent $50 million settlement by a West Virginia hospital shows the danger of violating or skating on the edge of federal laws regarding kickbacks. It also shows the vulnerability of healthcare organizations to current and former employees who are willing to allege wrongdoing to get a piece of the recovered funds.

The Department of Justice (DOJ) alleged that from 2007 to 2020, under the direction of its prior management, the hospital systematically violated the Stark Law and Anti-Kickback Statute (AKS) by "knowingly and willfully paying improper compensation to referring physicians that was based on the volume or value of the physicians' referrals or was above fair market value."

> THE CASE IS YET ANOTHER REMINDER TO HOSPITALS OF THE IMPORTANCE OF STRUCTURING PHYSICIAN COMPENSATION ARRANGEMENTS IN A MANNER THAT IS CONSISTENT WITH FAIR MARKET VALUE.

A former executive vice president filed a whistleblower complaint in 2017 under the qui tam provisions of the False Claims Act (FCA), which allow individuals to bring a lawsuit on behalf of the government and share in the proceeds. The employee had expressed concerns about the arrangement and then was fired for not cooperating with it, according to the DOJ. The whistleblower will receive $10 million of the $50 million settlement.

ReliasMedia.com

Financial Disclosure: Author **Greg Freeman**, Editor **Jill Drachenberg**, Editor **Jonathan Springston**, Editorial Group Manager **Leslie Coplin**, Accreditations Director **Amy Johnson, MSN, RN, CPN**, and Nurse Planner **Maureen Archambault**, RN, MBA, HRM, CPHRM, FASHRM, 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:
(800) 688-2421.
customerservice@reliasmedia.com
ReliasMedia.com

In support of improving patient care, Relias LLC is jointly accredited by the Accreditation Council for Continuing Medical Education (ACCME), the Accreditation Council for Pharmacy Education (ACPE), and the American Nurses Credentialing Center (ANCC), to provide continuing education for the healthcare team.

The 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 the activity.

1.5 ANCC contact hours will be awarded to participants who meet the criteria for successful completion. California Board of Registered Nursing, Provider CEP#13791.

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

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

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 DIRECTOR: Amy M. Johnson, MSN, RN, CPN

This settlement is among the pantheon of recent significant settlements with hospitals concerning alleged FCA violations predicated on violations of the Stark law and the AKS, says **Travis Lloyd**, JD, partner with Bradley in Nashville, TN. It reflects the government's continued emphasis on combatting healthcare fraud. It is yet another reminder to hospitals of the importance of structuring physician compensation arrangements in a manner that is consistent with fair market value and does not take into account, directly or indirectly, the volume or value of physician referrals, he says.

The alleged misconduct in this case is fairly straightforward, Lloyd explains. Among other things, the hospital allegedly paid physicians far in excess of fair market value and tied incentive compensation to the net revenue attributable to physicians, including technical fees billed by the hospital in connection with the physicians' services.

Two features of the settlement stand out to Lloyd. First, the hospital was not required to enter into a corporate integrity agreement in connection with the settlement — a difference from prior settlements concerning similar allegations. This likely reflects the fact that a new operator took over the management of the hospital shortly after the government intervened in the case, he says.

"The case also is remarkable for the fact that the defendant hospital filed a countersuit against the relator, a former executive vice president of the hospital, in which it alleged that the relator breached his fiduciary duty to the hospital by not reporting and attempting to prevent the misconduct in the qui tam action," he says.

The hospital dropped that suit shortly after filing it in 2019.

Hospital Should Have Known

The most surprising thing about the case is that it happened at all, says **Ericka L. Adler**, JD, shareholder with Roetzel & Andress in Chicago. There is a wealth of past cases and instructions from regulators regarding this type of fraud allegation, she says.

The case might not have been a surprise if it occurred 10 years ago when the rules were not quite as clearly defined, she explains, but now there is no excuse for now for the kind of arrangement alleged by the DOJ.

Adler often is involved with contracts in which entities are negotiating similar arrangements. She says they always rely on compliance language to ensure they meet the legal requirements for fair market value. When Adler negotiates physician contracts, she finds the hospital

EXECUTIVE SUMMARY

A hospital's $50 million settlement over kickback allegations holds lessons for hospitals. The hospital allegedly paid physicians for more than fair market value.

- A healthcare appraisal firm should determine fair market value.
- A physician compensation committee is an essential part of oversight.
- Billing errors and omissions insurance are available.

usually is quite rigid about following valuations. Even if she thinks the valuation is too long, the hospitals often are so risk-averse they usually will not yield.

"If one party doesn't like it, too bad, because the hospital is not going to take the risk of noncompliance. The fact that this happens tells me it involved people who didn't think they were going to get caught and that everyone was on the same page about it being a good deal for both sides," she says. "The doctors were happy and getting a lot of money, fairly greedy. I found it kind of shocking because I thought everyone knew that this was not acceptable, not likely something they would get away with, and there have been so many other identical situations where people got in trouble."

The case also illustrates the danger of whistleblowers, Adler says. The days of hiding shenanigans by threatening or firing employees who have the dirt on the company are long gone.

"No matter how small or big you are, where you are located geographically, how loyal you think your people are, you're likely going to get caught," Adler says. "They assumed their team was on the same page and ignored any complaints or concerns, thinking they won't be the ones to get caught."

Adler notes the physicians in this case were operating at a loss, yet still commanded extraordinarily high compensation from the hospital. That suggests an arrangement that would go beyond any fair market value compensation, she says.

"There are gray areas because fair market value is not an exact number, but this seemed egregious, that there was no reasonable way people would think this was going to pass the smell test," Adler says. "This wasn't offering them just a little bit above fair market value and you can say that's not a big deal."

Physicians may not be intimately familiar with Stark and AKS, and will readily accept a very high compensation, Adler notes.

"I talk about that with my clients. Almost every time, it's like they're hearing about it for the very first time, especially with the younger doctors," Adler says. "If an offer that is obviously unreasonable comes through, I put the blame on the compliance people in the hospital because they are the ones who should be aware of this. In this case, I'm shocked the doctors' lawyers didn't say something and tell them it was too good to be true."

"NO MATTER HOW SMALL OR BIG YOU ARE, WHERE YOU ARE LOCATED GEOGRAPHICALLY, HOW LOYAL YOU THINK YOUR PEOPLE ARE, YOU'RE LIKELY GOING TO GET CAUGHT."

The allegation about the hospital firing the executive vice president for questioning the compensation program was especially concerning. "If the whistleblower's allegations are to be believed, they did just about everything wrong here," Adler says.

In many cases, the hospital gambles on the fact that many employees who could file a qui tam lawsuit will not do so because of the potential risk to reputation and loss of employment.

"I think that's common, and some employers count on it. Employees who have knowledge of wrongdoing look at the potential payoff, and that can be huge, but they also look at what might happen if it goes nowhere and they've ruined their careers," Adler says. "In this case, you had someone who followed through."

The determination of fair market value compensation is key to this case. It appears the hospital did not follow accepted procedures, says **Rob Fuller**, JD, partner with Nelson Hardiman in Los Angeles.

Fair market value is a safe harbor against kickback allegations, Fuller explains. There is some wiggle room when determining that value.

The hospital can test the wind as to what fair market value is, but cannot be so far out as to pay double or triple the market rate. "If you paid them 120%, no one would be upset; that would just be super-high market value. You can't go way beyond that and plead ignorance, because there are plenty of resources for both nationwide and regional standards," Fuller says. "They were pretty callous and just figured they would never get caught. A hospital administrator in this day and age is not unaware of the Anti-Kickback Statute and the personal services safe harbor."

Informed Employees Can Blow Whistle

Part of what makes the FCA so dangerous is lawsuits can be brought by anyone with information about the arrangement, notes **Scott Bennett**, JD, an attorney with Coppersmith Brockelman in Phoenix.

"Many False Claims lawsuits have been brought by insiders, including hospital executives, compliance officers, and even in-house attorneys.

This case highlights the need for hospitals to not just have compliance programs on paper, but to put them into practice," he says. "There should be mechanisms in place to make sure that people are comfortable reporting potential legal violations, and that the hospital thoroughly investigates and responds to all concerns — even if those concerns relate to physicians who generate a lot of business for the hospital."

There were allegations that an internal hospital memo stated the hospital's physician practices were operating at a loss because of the high salaries paid to physicians. The DOJ has taken the position that a hospital losing money on a physician practice indicates the compensation is more than fair market value, Bennett says. Although that is debatable as a legal matter, he says, hospitals should take a hard look at any arrangement where they are losing money on physicians to ensure the arrangement complies with the Stark Law and AKS.

"The best way for hospitals to ensure that the compensation they are paying physicians is legally compliant is to get a fair market value opinion regarding the compensation from a healthcare appraisal firm," Bennett says. "Hospitals should also do their own ballpark comparison of physicians' compensation to benchmarks such as MGMA surveys of physician compensation."

Assign Responsibility for Oversight

Hospital systems avoid overpaying physicians by assigning responsibility for oversight of physician compensation and by following well-defined processes for setting and approving each compensation arrangement, says **Keith A. Smith**, JD, an attorney with Moore & Van Allen in Charlotte, NC. Specifically, Smith says a hospital system should use a physician compensation governance structure, a written compensation policy succinctly documenting the system's compensation philosophy, objectives, and robust internal controls.

"Optimal governance structure includes a physician compensation committee, with physician and nonphysician members who do not have management responsibility for running the physician practices, operating under a charter and with authority delegated by the hospital system board," Smith says. "The compensation committee should be charged with approving the standard physician compensation arrangements and any variations from those established standards."

The hospital system's corporate compliance team should regularly review and audit the physician compensation program's internal controls, which include rules, policies, and procedures for determining fair market value, commercial reasonableness, and when to engage external compensation experts, Smith says.

Health systems mitigate the risk of physician compensation arrangements running afoul of fraud and abuse laws by establishing a physician compensation governance structure, a compensation philosophy, and internal controls. "Using these formal structures, a health system sets clear lines of responsibility and accountability for maintaining a compliant physician compensation program," Smith advises.

Risky Game to Play

The payment of excessive compensation to patient referral sources is risky, says **Geoffrey R. Kaiser**, JD, partner with Rivkin Radler in Uniondale, NY. Stark prohibits a physician from referring patients for certain categories of "designated health services" (such as laboratory testing or imaging services) to any entity with which the referring physician has a prohibited financial relationship. The AKS prohibits the payment of anything of value for the purpose of inducing the referral of patients for the provision of any item or service reimbursable under a federal healthcare program.

Stark is a civil law and a strict liability statute under which knowledge and intent are not relevant to liability, Kaiser explains. The AKS is a criminal statute under which the prohibited activity must be knowing and willful to trigger liability. Both statutes include certain exceptions for qualifying arrangements with employees and independent contractors.

"However, under Stark, all of these exceptions require that the financial relationships be commercially reasonable and fair market value without taking into account the volume or value of referrals. Under the AKS, the same requirements apply to personal services arrangements with independent contractors," he says.

To be protected under the AKS employee safe harbor, the compensation paid must be for employment in the furnishing of items or services reimbursable under a federal healthcare program. While the safe harbor does not reference fair market value or commercial reasonableness, paying employees for their referrals would be viewed with suspicion by many courts, Kaiser says.

"In short, a hospital may not pay excessive compensation to its physicians as an incentive for patient

referrals without risking liability under these laws," he says.

Complicated Web of Laws

This case emphasizes the healthcare business is much more complicated that what happens at the bedside, says **Rochelle Sweetman**, JD, risk management consultant with Marsh & McLennan Agency in Sioux Falls, SD. Healthcare providers, physician groups, facilities, and systems, as well as drug and device manufacturers, laboratories, and insurers are governed by a complicated web of federal, state, and local regulations, she notes.

From the federal perspective, Stark, the AKS, and the FCA provide frameworks for the DOJ to bring enforcement actions against healthcare entities, Sweetman says. In 2019 alone, the DOJ recovered more than $2.6 billion in healthcare fraud claims. For the last 10 years, recoveries from the healthcare industry have exceeded $2 billion each year, she notes.

Sweetman notes defending cases brought by the government can be extremely expensive. In addition to the potential for refunding any overpayments, healthcare entities incur expenses from defense attorneys, as well as forensic accounting and audit expenses. Most significantly, they may be subject to civil fines and penalties imposed by the government, which often seeks exemplary damages in multiples of the alleged amount of fraudulent payments, she says.

Billing Insurance Available

An important lesson from this case is the commercial availability of billing errors and omissions (E&O) insurance, Sweetman says. Healthcare entities may find some billing E&O coverage in their directors' and officers' policies, but often the amount of available coverage is limited. In light of the demand for such coverage, insurers have developed standalone billing E&O policies.

"These policies can help cover the legal expenses to defend an allegation of billing impropriety, as well as associated fines and penalties, although not disgorgement — the return of payments improperly received," she says. "In addition, coverage may be available for the expenses of voluntarily disclosing billing issues to the government prior to any government action. Some billing E&O policies also cover claims brought by commercial payers, further helping healthcare entities protect their balance sheet from fraudulent billing claims." ■

SOURCES

- **Ericka L. Adler**, JD, Shareholder, Roetzel & Andress, Chicago. Phone: (312) 582-1602. Email: eadler@ralaw.com.
- **Scott Bennett**, JD, Coppersmith Brockelman, Phoenix. Phone: (602) 381-5476.
- **Travis Lloyd**, JD, Partner, Bradley, Nashville, TN. Phone: (615) 252-2306. Email: tlloyd@bradley.com.
- **Rob Fuller**, JD, Partner, Nelson Hardiman, Los Angeles. Phone: (312) 203-2803. Email: rfuller@nelsonhardiman.com.
- **Geoffrey R. Kaiser**, JD, Partner, Rivkin Radler, Uniondale, NY. Phone: (516) 357-3161. Email: geoffrey.kaiser@rivkin.com.
- **Keith A. Smith**, JD, Moore & Van Allen, Charlotte, NC. Phone: (704) 331-2375. Email: keithsmith@mvalaw.com.
- **Rochelle Sweetman**, JD, Risk Management Consultant, Marsh & McLennan Agency, Sioux Falls, SD. Phone: (605) 339-3874. Email: rochelle.sweetman@marshmma.com.

Privacy Concerns with Telehealth Should Prompt Review

With the use of telehealth increasing in response to the COVID-19 pandemic, there is growing concern the technology may pose risks to patient privacy. In particular, any telehealth services quickly established at the beginning of the pandemic may need a close review to ensure they do not result in data breaches.

While telehealth has captured a lot of attention since COVID-19, most of it has been focused on the changes to the care delivery model, such as the safety, convenience, and ability to provide some basic care remotely, notes **David Finn**, executive vice president for strategic innovation with CynergisTek, a cybersecurity consulting firm based in Austin, TX.

"From a technology perspective, it has focused on what providers need to do and the relaxation of certain rules related to physician credentialing, reimbursement, and what will remain of these changes as we return to something that looks more like our pre-COVID-19 world of healthcare," he says. "We seem to have missed what is important to the people that all of this was done for — the patients."

CynergisTek recently conducted a survey to address the emerging security and privacy concerns of patients who opted for phone and video consultations over in-person visits during a recent period. Seventy-three percent said they plan to continue to use telehealth.

Finn notes these other results from the survey:

- 79% of male respondents who have used a telehealth solution during the COVID-19 pandemic will continue using them post-COVID, compared to 67% of females.
- 81% of millennials will continue to use telehealth options after the pandemic, as will 79% of Gen X respondents.
- 25% said they would not consider using a telehealth solution for any of the hypothetical appointments or procedures presented. That number is significantly higher among baby boomers at 41% and the Silent Generation (those born from 1928 to 1945) at 59%. *(More information is available at: https://bit.ly/33K2xq5.)*

Patients Willing to Use Telehealth

Healthcare has clearly discovered a real opportunity, Finn says. Americans will look to telehealth to fill the gap for routine types of care. For example, nearly 30% of survey respondents would look to telehealth for chronic care check-ups or annual physical and children's wellness exams.

"This is where it gets tricky for providers. We know from weekly incidents in the media and studies of the industry that privacy and security are lagging in the healthcare sector," he says. "While patients are ready to embrace telehealth, providers most prioritize privacy and security when rolling out phone or other virtual services. If they don't, they run the risk of potential breaches of sensitive and often legally protected patient information."

Healthcare providers need to reassess and strengthen their security to reflect this new reality or potentially risk losing their patients' trust and business, Finn says. He cites this further evidence from the survey:

- 48% of respondents said they would be unlikely to use telehealth if their personal health data was compromised.
- 54% of women indicated they would not use telehealth solutions again if their health information was compromised in a breach, vs. 41% of men.
- Baby boomers and the Silent Generation are the least likely to return to telehealth solutions if their data were compromised (62% and 65%, respectively).

Responses also indicated that the older the group, the less likely they were to have the technology, skills, and capabilities to use these telehealth tools. However, these groups would most benefit from these types of services, Finn notes.

The first step any health system can take to ensure patient privacy is to understand the potential risks

EXECUTIVE SUMMARY

As the use of telehealth increases, so do concerns over patient privacy. Best practices can reduce the risk of data breaches.

- Conduct a risk analysis on telehealth services.
- Closely review any programs hastily set up as a response to COVID-19.
- Limit the use of telehealth to appropriate settings and uses.

and vulnerabilities that exist when protected health information (PHI) is transmitted electronically, says **William P. Dillon**, JD, shareholder with Gunster in Tallahassee, FL. These risks and vulnerabilities can be learned by conducting a robust risk analysis of the health system's processes for creating, receiving, maintaining, and transmitting PHI, he says.

"A risk analysis allows a covered entity to know what it is doing right — and more importantly, lets the covered entity know which areas need improvement. It is the failure to mitigate known deficiencies that still seems to be a big issue for many in healthcare," Dillon says. "Only by properly securing ePHI can patient privacy be maintained with any level of confidence."

Along with proper security measures required by the HIPAA security rule, one best practice is to learn how PHI moves through an organization, Dillon says. He notes the Department of Health and Human Services Office for Civil Rights (OCR) Summer 2020 Cybersecurity Newsletter focused on the importance of a covered entity understanding the IT assets that are under its control. *(The newsletter is available at this link: https://bit.ly/2IcNkpo.)*

For example, the covered entity should be aware of both its hardware and software assets, Dillon explains. Once aware of its assets and how they are interconnected, the covered entity should ensure all known vulnerabilities are patched and/or otherwise remediated.

It is imperative to maintain that required privacy mindset, Dillon says. A healthcare provider can engage in a telehealth session on a device that is fully secure, but if that telehealth session is conducted in an area where unauthorized people can see or hear the interaction, the patient's privacy is subject to compromise, he explains.

"Another pitfall or mistake would be to make sure that any technology that is being used for telehealth is not public-facing," he says. "While OCR has indicated that it will exercise enforcement discretion during the COVID-19 crisis, it has specifically warned providers not to utilize communication applications such as Facebook Live, Twitch, and TikTok for patient communications."

While more patients are aware of telehealth than ever, concerns remain about how the process works and how information is collected, Dillon says. One of the best ways to deal with these concerns is through patient education. Many healthcare providers require providing patients with a document similar to an informed consent form. Such documents outline how telehealth works and the pros and cons of the telehealth option, he says.

Respect Patient Concerns

Patient privacy is a valid concern with telehealth, and one that each healthcare provider and patient should take seriously, says **Jay Backstrom**, vice president at Impact Advisors, a healthcare consulting firm based in Boston. Concerns about internet privacy in general have spiked in recent years due to incidents of data breaches and internet fraud. Many patients are worried about the security of their personal information.

"Many patients are accustomed to seeing their healthcare provider in a private patient room, so perceptions about privacy are a greater concern with many more patients now having a similar visit via telehealth," he says. "Secure connections and data encryption help protect information during telehealth visits, but many patients will want more assurances to ease their concerns. Patients should be asking their clinical provider how their privacy is being protected."

Clinical care providers should continue to adhere to defined HIPAA requirements, and use HIPAA-enabled telehealth applications and videoconferencing platforms. Patient privacy and data protection policies should be established and made accessible to patients before their telehealth visit, he says.

"Additionally, clinical staff should be instructed to follow a defined process for performing all telehealth visits to ensure patient privacy is protected. The process should include functional, operational, and technical protections for patient privacy and data captured during and after the clinical encounter," Backstrom says. "For example, before clinical care is provided, the care team should verify the identity of the patient. If it is a follow-up visit, have the patient validate some of his or her previous encounter information."

Telehealth Best Practices

Backstrom recommends these telehealth best practices:

- Only use telehealth applications and videoconferencing platforms that meet HIPAA privacy and data security requirements.
- Ensure all telehealth staff receive HIPAA security training and only authorized providers have access to patient data.
- Establish patient privacy and data protection policies and provide patients access to these policies before their telehealth visit.

• Ensure telehealth application data is encrypted and protected.

• Use telehealth applications that require a login and password for all users.

• Integrate the electronic medical record with the telehealth platform for bidirectional information exchange to ensure a single source of record for the patient.

Patients also can take steps to protect their own devices against security and privacy risks for a telehealth visit or anything involving their online personal data, Backstrom notes. Patients should verify they are using a secure website (shown by the "lock" icon in the browser's address bar), make sure their wireless connection is secure and password protected, and ensure they have an up-to-date antivirus software running on their computer.

"If you follow the best practices, then you will avoid many of the common mistakes. Beyond the best practices, clinical providers should avoid outdated views of patient privacy and data protections that shifts the responsibility to someone else," Backstrom says. "Everyone who interacts with the patient through telehealth has a vital role to play in the protection and privacy of the patient's information, including the patient."

Treat Like Other Healthcare Services

Telehealth services still are healthcare services, and most of the compliance issues will look familiar, says **Roy Wyman**, JD, partner with Nelson Mullins Riley & Scarborough in Nashville, TN. A risk manager will want to ask if the proper services actually were provided, if they were billed correctly, and whether there are any problematic referral or compensation relationships, among other concerns.

"The compliance program for telehealth should look like the broader program: involve a risk assessment, risk management plan, benchmarking, auditing and monitoring, and more on a regular cycle," he says. "New elements to address telehealth specifically may need to bring special attention to the relationship between any telehealth management or platform services and the physicians. Of particular concerns are the corporate practice of medicine, inappropriate compensation relationships, fee-splitting, and IT security concerns."

The concerns are valid because attacks on the privacy and security of health information are increasing, Wyman says. Keep in mind there are two different aspects where privacy can be a concern. The first is when actually communicating as part of treatment. The second is when the provider accesses and stores the records of that treatment.

Each has unique risks, and the provider should speak to how they protect data in both those settings, Wyman says. Regarding the treatment itself, many providers are new to the telehealth space and may not bring enough knowledge and investment to make sure their systems are secure.

Wyman notes while relaxation of Medicare rules may permit using a broader range of platforms in providing telehealth, the hospital or system still must comply with HIPAA and avoid undue risks to patient privacy. That includes undertaking a risk assessment.

"That assessment should include a review of the overall security of the transmission and storage of PHI. Proper security, at a minimum, should include a review of the telehealth platform, involve additional training for providers and anyone accessing the system, and consider the level of security of the data being transmitted," he says. "Other requirements of HIPAA security rules also apply and will involve things like access controls to determine how users are verified, integrity to assess ways of confirming the reliability of data, logging of data and identifying system intruders, availability of the data, and other concerns."

Ensuring a secure telehealth program comes back to the common elements of any effective compliance program, Wyman says. That includes a team that can get the attention of others in an organization and has a regular compliance cycle, usually annual, he says. It also will include a thorough risk assessment (often undertaken by an outside contractor), a risk management plan, benchmarking, and auditing/monitoring.

"With regard to telehealth specifically, the program must address issues regarding training, coding, collection of information, proper contracting, and making sure that there are no improper ownership or referral relationships," he says.

A common mistake is jumping into telehealth without any experience or understanding of the risks, Wyman says. For example, providers may be tempted to just start taking Zoom calls from patients and billing it.

"When the system breaks, or the unexpected happens, there isn't a plan to address it. Likewise, simply signing up with a telehealth platform without consulting and legal assistance creates risks. If the system is hacked, or the platform breaks its promises, will the provider have any recourse against the

platform?" Wyman asks. "Has there been due diligence to make sure that the platform is established and reliable? Are the providers trained, and do they understand the unique challenges of telehealth regarding coding, follow-up, and the provider-patient relationship at a distance? Will the system still work when and if we go back to the old rules from pre-COVID-19?" ■

SOURCES

- **Jay Backstrom**, Vice President, Impact Advisors, Boston. Phone: (800) 680-7570.
- **David Finn**, Executive Vice President, Strategic Innovation, CynergisTek, Austin, TX. Phone: (512) 402-8550.
- **William P. Dillon**, JD, Shareholder, Gunster, Tallahassee, FL. Phone: (850) 521-1708. Email: wdillon@gunster.com.
- **Roy Wyman**, Partner, Nelson Mullins, Nashville, TN. Phone: (615) 664-5362. Email: roy.wyman@nelsonmullins.com.

Malpractice Risks of Telehealth Still Being Determined

Risk managers should be wary of the malpractice risks associated with telehealth, according to several experts who say the sudden increase in usage may have introduced insufficiencies that should be assessed now.

Although the risk of malpractice in telemedicine is low, there are areas of concern when it comes to the malpractice risk in telehealth, says **Paul F. Schmeltzer**, JD, an attorney with Clark Hill in Los Angeles. The practice of medicine across state lines is one potential issue.

Physicians delivering care through telehealth should be careful to avoid practicing medicine in a patient's home state without being licensed in that state. In the case of most hospitals and physicians, this is generally not an issue, Schmeltzer says. However, providers should be aware of where their patient is receiving telehealth services before proceeding with the appointment.

Negligence claims from online prescribing are not uncommon, Schmeltzer notes. Some physicians who prescribe medications have faced liability for practicing medicine in a patient's home state without being licensed in that state.

"Some states, such as California, require doctors to have a pre-existing relationship with a patient in order to engage in online prescribing. In those states, the physician should understand how that state defines a relationship," he says. "Other states require a face-to-face physical exam prior to online prescribing. I would advise physicians to meet or communicate directly with the patient before prescribing medication."

To reduce their liability for malpractice, Schmeltzer says physicians should maintain records that establish an appropriate relationship with the patient, that the physician was able to properly assess the patient, and the patient has provided the physician with an accurate health history.

"Physicians also need to know the informed consent requirements for every state whose residents they treat," Schmeltzer says. "Otherwise, the physicians open themselves up to a potential lawsuit for treating someone without first obtaining informed consent."

Schmeltzer notes telehealth is not appropriate for conditions that require a physical examination. Elderly patients may benefit from in-person visits vs. telehealth for assessments or other patient care visits.

"In malpractice claims from telemedicine, the most common allegation has been a missed diagnosis, and the most commonly missed diagnosis was cancer," he says. "Physicians should also be aware that missed diagnoses for strokes, infections, and orthopedic concerns are not uncommon."

How can hospitals be confident the care delivered through telehealth is equivalent to care provided in person? **Thomas Davis**, MD, a consultant and expert witness in St. Louis, says they cannot.

EXECUTIVE SUMMARY

The malpractice risks of using telehealth are a growing concern for risk managers. Some risks are known, but the growing use of this technology may reveal new concerns.

- Negligence claims from online prescribing are not uncommon.
- Telehealth is inappropriate for some examinations.
- Missed diagnoses are the most common allegation in telehealth.

"Telemedicine is not, and, absent full telepresence technology that transmits touch and smell, will never be the equivalent of an in-person encounter. The spectrum of conscious and subconscious sensory information transmitted both ways during a telemedicine encounter is a fraction of that transmitted in an in-person encounter," he says. "In addition, very few clinicians have formal training in the virtual delivery of healthcare. My residency in family medicine at the University of Missouri-Columbia is one of the few."

Davis notes a med-mal lawsuit requires the patient not only be harmed in such a way that the financial value of the case is attractive to a plaintiff's attorney, but also the patient is angry enough to initiate the case. If the patient feels connected with the physician and cared for human-human, the chances of a lawsuit are much lower.

"Telemedicine greatly reduces the opportunity to make that connection, and greatly increases the chances of a suit-filing should a bad enough outcome occur," he says.

The greater the chance for an actionable outcome, the greater the redundancies that need to be constructed into the care systems. "Unfortunately, most health systems are designed to strip-mine healthcare dollars through an industrial delivery model," Davis says. "As such, they are seeing telemedicine as simply a way to turn up the treadmill. That's a recipe for disaster — for them and their patients."

Use Systematic Approach

The best way to ensure the quality of care provided through telehealth is to use a systematic delivery approach with lots of documented evidence of training and acknowledgement of understanding on the part of the provider, Davis says. He suggests including these items:

- **Hard stop check boxes.** "If an actionable outcome occurs and the provider can be shown to have checked a box inappropriately, the organization can deflect liability back to the provider," he says. "The benefit of this approach varies with the relationship of provider and employer."
- **Hard guidelines with specific instructions and mechanisms to address deviations during the encounter, such as when to send someone to the emergency department.**
- **Compensation systems that do not disincentivize clinicians from conservative treatments as appropriate**. For example, do not punish the clinicians financially for referring to the emergency department.
- **Formal training in "encounter hygiene," such as using persuasion and influence tactics to create the simulacrum of a patient connection.** The physicians should introduce themselves and establish their credentials at the very start of the encounter.
- **Make sure the patient sees a professional photo of the clinician even during an audio encounter.**

Right Policies and Procedures

Telehealth services should use an organized structure that is multidisciplinary and multispecialty, which provides oversight and approval mechanisms, says **Kim Pardini-Kiely**, associate director in the Clinical and Operational Excellence and Innovation Services practice with Protiviti in San Francisco.

Policies and procedures should define what is clinically appropriate care for telehealth services, as well as what is not, by specialty, she says. Evidence-based practices should be in place for prevention/wellness care, disease management, patient triage for urgent care, prescribing protocols, mental health counseling, and psychotherapy, and applied

consistently across all locations and by each provider.

The collection of patient monitoring data must include a process to evaluate and respond to the patient on treatment plans and any necessary modifications to the treatment plan, mitigating any risk for lack of follow-up, she says. Inclusion of Hospital Outpatient Quality Reporting indicators in The Joint Commission requirements for Ongoing Professional Practice Evaluation is a good mechanism for comparative data and oversight of the peer review process, Pardini-Kiely suggests.

There are specific types of care that should not be provided by telehealth, she says. Any care that would require an in-person physical exam would not be appropriate; however, a provider can determine during a telehealth visit that an in-person visit is necessary.

"Some of the best ways for ensuring the quality of telehealth care are through the collection and monitoring of patient satisfaction, disease-specific clinical outcomes, and prevention or wellness indicators that are tracked and compared to data collected for in-person visits, such as the Hospital Outpatient Quality Reporting by the Centers for Medicare & Medicaid Services," Pardini-Kiely says. ■

SOURCES

- Thomas Davis, MD, Tom Davis Consulting, St. Louis. Phone: (636) 667-6325. Email: tom@tomdavisconsulting.com.
- Kim Pardini-Kiely, Associate Director, Clinical and Operational Excellence and Innovation Services, Protiviti, San Francisco. Phone: (415) 402-3600.
- Paul F. Schmeltzer, JD, Clark Hill, Los Angeles. Phone: (213) 417-5163. Email: pschmeltzer@clarkhill.com.

CME/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 test 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.

CME/CE QUESTIONS

1. **In the West Virginia case in which the Department of Justice alleged violations of the Stark Law and Anti-Kickback Statute, how was the alleged fraud discovered?**

   a. A routine audit
   b. A whistleblower
   c. A report from the Centers for Medicare & Medicaid Services
   d. An accreditation survey

2. **Which is true regarding the West Virginia case, according to Ericka L. Adler, JD?**

   a. The hospital should have known the alleged arrangement was fraudulent.
   b. The hospital took all necessary precautions and it was reasonable to think the alleged arrangement was legitimate.
   c. The alleged arrangement might have been legitimate as recently as three years ago.
   d. There was no way for the hospital to know if the alleged arrangement was legitimate.

3. **In the survey by CynergisTek, what percentage of respondents said they would be unlikely to use telehealth again if their protected health information was compromised?**

   a. 18%
   b. 28%
   c. 48%
   d. 68%

4. **What does Paul F. Schmeltzer, JD, cite as one potential malpractice risk of telehealth?**

   a. Sessions that are too brief.
   b. The practice of medicine across state lines.
   c. Conveying direct medical instructions to a patient.
   d. Failing to obtain the patient's vital signs.

CME/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.

HEALTHCARE RISK MANAGEMENT™

DocuSign Envelope ID: 18B1968F-62D4-4649-ACCB-AC48BCBA015C

Statement of Ownership, Management, and Circulation
UNITED STATES POSTAL SERVICE® **(All Periodicals Publications Except Requester Publications)**

1. Publication Title	2. Publication Number	3. Filing Date
Healthcare Risk Management	1 0 8 1 – 6 5 3 4	10/1/2020
4. Issue Frequency	5. Number of Issues Published Annually	6. Annual Subscription Price
Monthly	12	$299

7. Complete Mailing Address of Known Office of Publication *(Not printer) (Street, city, county, state, and ZIP+4®)*: 1010 Sync St., Ste.100, Morrisville, NC 27560-5468. — Contact Person: Sabrina Johnson; (919) 459-9495

8. Complete Mailing Address of Headquarters or General Business Office of Publisher *(Not printer)*: 1010 Sync St., Ste.100, Morrisville, NC 27560-5468.

9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor *(Do not leave blank)*

Publisher *(Name and complete mailing address)*: Relias LLC, 1010 Sync St., Ste.100, Morrisville, NC 27560-5468.

Editor *(Name and complete mailing address)*: Jill Drachenberg

Managing Editor *(Name and complete mailing address)*: Leslie Coplin

10. Owner *(Do not leave blank. If the publication is owned by a corporation, give the name and address of the corporation immediately followed by the names and addresses of all stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, give the names and addresses of the individual owners. If owned by a partnership or other unincorporated firm, give its name and address as well as those of each individual owner. If the publication is published by a nonprofit organization, give its name and address.)*

Full Name	Complete Mailing Address
Relias LLC	1010 Sync St., Ste.100, Morrisville, NC 27560-5468.
Bertelsmann Learning LLC	1745 Broadway, New York, NY 10019

11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities. If none, check box → ☑ None

Full Name	Complete Mailing Address

12. Tax Status *(For completion by nonprofit organizations authorized to mail at nonprofit rates) (Check one)*
The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes:
☑ Has Not Changed During Preceding 12 Months
☐ Has Changed During Preceding 12 Months *(Publisher must submit explanation of change with this statement)*

PS Form **3526,** July 2014 *(Page 1 of 4 (see instructions page 4))* PSN: 7530-01-000-9931 **PRIVACY NOTICE:** See our privacy policy on *www.usps.com.*

DocuSign Envelope ID: 18B1968F-62D4-4649-ACCB-AC48BCBA015C

13. Publication Title: Healthcare Risk Management — 14. Issue Date for Circulation Data Below: September 2020

15. Extent and Nature of Circulation			Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Total Number of Copies *(Net press run)*			119	109
b. Paid Circulation *(By Mail and Outside the Mail)*	(1)	Mailed Outside-County Paid Subscriptions Stated on PS Form 3541 (Include paid distribution above nominal rate, advertiser's proof copies, and exchange copies)	99	94
	(2)	Mailed In-County Paid Subscriptions Stated on PS Form 3541 *(Include paid distribution above nominal rate, advertiser's proof copies, and exchange copies)*	0	0
	(3)	Paid Distribution Outside the Mails Including Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid Distribution Outside USPS®	1	1
	(4)	Paid Distribution by Other Classes of Mail Through the USPS (e.g., First-Class Mail®)	7	3
c. Total Paid Distribution *[Sum of 15b (1), (2), (3), and (4)]* ▶			107	98
d. Free or Nominal Rate Distribution *(By Mail and Outside the Mail)*	(1)	Free or Nominal Rate Outside-County Copies included on PS Form 3541	2	1
	(2)	Free or Nominal Rate In-County Copies Included on PS Form 3541	0	0
	(3)	Free or Nominal Rate Copies Mailed at Other Classes Through the USPS (e.g., First-Class Mail)	0	0
	(4)	Free or Nominal Rate Distribution Outside the Mail *(Carriers or other means)*	2	2
e. Total Free or Nominal Rate Distribution *(Sum of 15d (1), (2), (3) and (4))*			4	3
f. Total Distribution *(Sum of 15c and 15e)* ▶			110	101
g. Copies not Distributed *(See Instructions to Publishers #4 (page #3))* ▶			9	8
h. Total *(Sum of 15f and g)*			119	109
i. Percent Paid *(15c divided by 15f times 100)* ▶			97%	97%

* If you are claiming electronic copies, go to line 16 on page 3. If you are not claiming electronic copies, skip to line 17 on page 3.

DocuSign Envelope ID: 18B1968F-62D4-4649-ACCB-AC48BCBA015C

Statement of Ownership, Management, and Circulation
UNITED STATES POSTAL SERVICE® **(All Periodicals Publications Except Requester Publications)**

16. Electronic Copy Circulation	Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Paid Electronic Copies ▶		
b. Total Paid Print Copies (Line 15c) + Paid Electronic Copies (Line 16a) ▶		
c. Total Print Distribution (Line 15f) + Paid Electronic Copies (Line 16a) ▶		
d. Percent Paid (Both Print & Electronic Copies) (16b divided by 16c × 100) ▶		

☐ **I certify that 50% of all my distributed copies (electronic and print) are paid above a nominal price.**

17. Publication of Statement of Ownership

☑ If the publication is a general publication, publication of this statement is required. Will be printed in the November issue of this publication. ☐ Publication not required.

18. Signature and Title of Editor, Publisher, Business Manager, or Owner: DocuSigned by: Philipp Russcle 40074DA3CF8246E... — Chief Financial Officer — Date: 29-Sep-2020

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties).

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

Appeals Court Affirms $9.2 Million Noneconomic Damages Award in Medical Battery Case

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: In 2014, a patient underwent surgery to remove a mass on his scrotum. After discovering the mass was larger than expected, the physician removed a greater portion of tissue than the patient wanted. The physician did not obtain informed consent from the patient (who was under anesthesia) or of the dedicated medical proxy. The invasive surgery caused severe side effects and irreversible injuries. The patient filed a lawsuit alleging malpractice and medical battery.

The trial court ruled in favor of the patient and awarded $9.2 million in noneconomic damages. On appeal, the defendants argued the award must be reduced to conform with the state's $250,000 cap on noneconomic damages. However, the appellate court affirmed the trial court's decision and stated certain medical battery claims are exempt from the statutory maximum.

Background: In 2014, a 41-year-old man discovered a small mass on his scrotum. The patient sought medical attention, stating he experienced some mild scrotum pain. He explained he did not experience dysfunction or pain in his penis, and reported he was sexually active. After consulting with a physician, the patient agreed to undergo surgery to remove the mass and send it for a biopsy. The surgery was to be performed under general anesthesia, but was supposed to be minimally invasive as an outpatient surgery. The patient was informed as to the possibility of infection, swelling, discomfort, and injury to the surrounding tissue.

THE PHYSICIAN KNEW THE PROCEDURE WOULD RENDER THE PATIENT IMPOTENT, BUT NEVERTHELESS DECIDED TO PROCEED.

The physician described the surgery as requiring a small incision to remove the mass, which was expected to be approximately 1 cm. The patient completed the informed consent forms and identified his ex-wife as his medical proxy to make medical decisions for him while he was under anesthesia, if necessary. On the day of the surgery, the patient's ex-wife was present at the hospital and remained available throughout the procedure. As the physician made the incision, he discovered the mass was much larger than originally expected and that it spread to the patient's penis. The physician observed that the mass was vascularized and involved the patient's nerves, and he believed the mass was malignant.

Instead of taking a portion of the mass to send to biopsy, the physician decided to remove the entire mass, which measured 8 × 5 × 2.5 cm. The physician knew the procedure would render the patient impotent, but nevertheless decided to proceed. Furthermore, the physician admittedly failed to read the forms with the designation of the patient's medical proxy. The physician allegedly was unaware the patient's proxy was present at the hospital and did not obtain her consent. The mass turned out to be a benign cystic lymphangioma.

A few weeks after the surgery, the patient sought

emergency medical treatment for an infection that caused boils with drainage and causing excruciating pain. Additionally, the patient became completely impotent after the surgery and suffered from constant pain internally at the base of his penis, loss of feeling, and difficulty urinating. After two reconstructive surgeries, the patient regained some function in his penis and claimed the level of pain was tolerable. However, touching or moving the penis caused severe pain, and sexual intercourse was extremely painful.

The patient brought a claim against the physician and the hospital, alleging medical malpractice and medical battery. The defendants denied liability. A jury awarded the patient $9.25 million in noneconomic damages. The defendants appealed the award, arguing the state's maximum on noneconomic damages limited the permitted award to $250,000. However, the appellate court affirmed the award, as medical battery is legally distinct from medical malpractice, and the maximum only applied to malpractice causes of action.

What this means to you: The most important lesson for physicians and care providers from this case is to always receive fully informed consent for the actual procedure performed. Receiving consent beforehand is a prerequisite, but if the circumstances change, or if a modification to the procedure appears appropriate, seek and receive consent again. Fully informed consent, wherein the patient is advised of the details of treatment, the potential risks, and possible alternative treatment options, is critical to preventing malpractice claims. While this is a common practice, asking a patient to read, understand, and sign consent forms protects from later claims by a patient who may, years down the line, argue he or she was not informed of the risks.

Another interesting legal lesson from this case is the nuanced distinction between a medical malpractice cause of action and a medical battery cause of action. Malpractice occurs when a physician fails to use the level of skill, knowledge, and care a reasonably careful physician would use in the same or similar circumstances. Medical battery occurs when a physician performs a procedure without consent, or the patient consented to one procedure but the physician performed a substantially different surgery. It is thus possible for a physician to act negligently by failing to adequately disclose risks and alternatives, but the patient nevertheless consents to the procedure. By contrast, if the patient provides no consent or the physician diverges from the agreed-upon procedure, that is medical battery.

A single set of facts may constitute both malpractice and battery, and it can be a fine line to argue whether the procedure "substantially" differed from the consent provided. Expert testimony may prove critical to persuading a jury that any variance was minor and not substantial. This distinction is critical because, as demonstrated in this case, if the jury determines the deviation to be substantial, it may constitute battery and not be subject to the statutory maximum. If the difference is minor, then statutory maximums apply, leading to a difference of an adverse verdict of $250,000 or exponentially more, as this $9.25 million award reveals.

For this reason, some courts have clarified the cap on noneconomic damages should not be applied as a clear-cut rule where only causes of action brought under the standard of negligence would fall within its scope. Rather, a patient's claims must be analyzed based on the facts of the case. In this case, the court of appeals elaborated on this concept, providing that where a physician merely exceeds the scope of the consent provided by the patient, the claim will be subject to the $250,000 noneconomic damages cap. However, in cases in which the medical professional obtains consent for one procedure but performs a completely different one, the breach of the patient's consent will constitute medical battery and will be exempt from the limitation on damages.

Here, the court found the patient's cause of action under negligence was clear in several respects. First, the physician admitted to failing to fully read the consent form, which led to his lack of awareness as to the patient's medical proxy, who was in the building at the time of the procedure. Secondly, the physician's decision to remove the entire mass was negligent because the physician testified the risks to the patient's urethra, even if the mass was malignant, would occur weeks, if not months, after the surgery. Under these circumstances, waiting one week to perform a biopsy would have been justifiable and safe. The physician also expressed concern that scarring from the first surgery may have caused problems if the mass was removed at a later stage. However, the physician admitted this opinion was speculation. Therefore, the court affirmed the finding of malpractice.

Regarding the medical battery claim, the court stated these events clearly constituted an episode exempt from the noneconomic damages cap because the physician did not merely exceed the consent he had obtained. Rather, he performed a completely

different and separate procedure to which neither the patient nor his proxy had consented. Specifically, the patient agreed to a short outpatient procedure during which a small, 1 cm mass would be removed from his scrotum to obtain a biopsy. Instead, the patient underwent a much more invasive procedure, during which a much larger mass was extracted from both his scrotum and his penis, rendering him impotent and causing him severe physical and emotional pain. Accordingly, the court confirmed the physician committed both malpractice and battery, subjecting him to damages in excess of the statutory maximums. ■

REFERENCE

Decided on Sept. 10, 2020, in the Court of Appeal of the State of California, Fourth Appellate District, Case Number E071146.

Court Rules Defendants Must Face Malpractice Suit After Botched Delivery, Death of Twin

News: In 2016, a woman was 27 weeks pregnant with twins. In the final stages of her pregnancy, she visited a physician four times to address abnormal discharge and abdominal pain, but was sent home each time. Less than three days after her final visit, the patient returned to the hospital in labor and gave birth to the first twin within 12 minutes of arriving. Due to complications during delivery, the premature baby suffered injuries that led to her death a month later.

During the subsequent malpractice action, the defendants challenged the sufficiency of the patient's expert report. However, an appellate panel rejected every claim the hospital raised as to the sufficiency of an expert report submitted by the patient. The court ruled the information in the report satisfied the requirements for admissibility of an expert report.

Background: In 2016, the 25-year-old patient was pregnant with twins. The patient gave birth to two children before becoming pregnant with these twins. From April 2016 to July 2016, the patient saw a physician for prenatal care visits. In April 2016, an ultrasound revealed each twin was healthy and the pregnancy was proceeding as expected. A second ultrasound was performed in early June, which again showed the twins were healthy.

Three weeks later, the patient returned to the physician for a follow-up visit that showed no abnormalities. However, five days later, the patient arrived to the hospital complaining about mucous discharge over the past five days, accompanied by abdominal cramps, diarrhea, and mild contractions. A different physician at the hospital examined the patient but did not observe any vaginal bleeding or fluid leakage, contractions, or pelvic pain. Further examination revealed the patient's cervix was not dilated. However, no scans or ultrasounds were performed.

The patient was sent home after receiving a concentrated electrolyte shot, and was instructed to follow up with her physician two weeks later. The hospital physician called the patient's physician to inform him of the situation. The patient's primary physician confirmed he would see the patient during the regularly scheduled appointment. Two days later, the patient returned to the hospital in labor. Within 12 minutes of her arrival, she delivered the first twin.

The hospital report indicated when she arrived at the hospital the amniotic sac was protruding and the patient presented bright red vaginal bleeding and heavy drainage with a foul odor. The first twin was in a breech position, which caused her head to get stuck in the patient's cervix for five minutes. After delivery, the baby's heart rate was low, she was blue, and was not breathing. She required immediate resuscitation. The baby was transferred to the neonatal intensive care unit, where she experienced seizures due to grade IV intraventricular hemorrhage on the left side of her brain and grade II intraventricular hemorrhage on the right side of her brain with post-hemorrhagic hydrocephalus. The second twin was delivered through an emergency cesarean section and also required intensive care for several weeks. However, in early August, the first twin died. The second twin's condition steadily improved until she was discharged.

The patient filed a medical malpractice action against multiple care providers: her primary physician (a gynecologist), the physician who examined her at the hospital, the nurse who assisted during delivery of the first twin, and the hospital that employed the medical staff. The defendants all denied liability and brought a motion to dismiss the case, arguing the patient's expert report was deficient. The trial court denied the defendants' motion, and they appealed the denial. The defendants

continued to argue the expert report was insufficient, but the court of appeals found in favor of the patient and affirmed the trial court's denial of defendants' motion to dismiss.

What this means to you: As with many medical malpractice cases, the primary issues in this case revolve around expert witnesses, who are almost always necessary and who can make or break a malpractice defense. Here, the defendants argued the report presented by the patient's expert was insufficient to establish a prima facie case of negligence because the expert was not qualified to opine on neurological injuries, and the report did not adequately address the issue of causation regarding the patient's physician. The hospital defendant also claimed the patient failed to provide sufficient evidence as to the hospital's breach of duty of care and causation.

The plaintiff's key evidence was the expert report prepared by a practicing gynecologist who explained how the medical staff failed to identify the preterm labor risk factors the patient started presenting in late June, failed to investigate whether the patient was about to enter preterm labor, and consequently failed to act to prevent preterm labor. Specifically, the expert opined preterm labor occurs before the 37th week of pregnancy.

In this case, the patient went into labor and delivered the twins when she was 27 weeks pregnant, which poses extreme risk to the infants since their organs are not fully developed. Furthermore, the expert opined that multiple gestation pregnancy is one of the known risk factors for preterm labor. Given this additional factor, the patient's physician should have been closely monitoring the patient for preterm labor symptoms once the twin pregnancy was confirmed through ultrasound in April 2016. The expert also alleged increased vaginal discharge, abdominal cramps with or without diarrhea, and contractions all were symptoms of preterm labor. Thus, when the patient arrived to the hospital complaining about these symptoms, her physician should have immediately ordered an ultrasound and monitored her closely to determine whether the patient was going into preterm labor.

Unfortunately, no ultrasound was performed. When alerted, the primary physician said he would see the patient during her scheduled appointment two weeks later. The patient was sent home after a concentrated electrolyte injection even though she clearly presented with symptoms of preterm labor. By failing to perform an ultrasound and investigate the patient's condition, the medical staff and physician breached their duty of care.

Moreover, according to the patient's expert, there are several methods to stop preterm labor, including bed rest, medications to stop contractions, and medications that help accelerate the development of the babies' organs. Had the defendants identified the symptoms of preterm labor, the patient could have continued the pregnancy for several weeks, and the babies would have been delivered in a safer manner, preventing the injuries and the death of the first twin.

There are several additional issues the physician and hospital could have managed and treated more appropriately. The foul-smelling discharge noted after the spontaneous delivery of the first twin required attention. A culture of the vaginal discharge should have been taken after the physician learned of its persistence. This might have shown the presence of chorioamnionitis, or infection within the uterus and amniotic fluid, which requires interventions such as antibiotics. Chorioamnionitis can cause preterm labor and delivery. Had an ultrasound been performed earlier, the presence of the breech presentation could have been anticipated by the staff present during the delivery.

To undermine these harmful expert opinions, the defendants argued that because the expert was not a neurologist, he was not qualified to opine as to the twins' neurological injuries. Additionally, because there was no guarantee that preterm labor would have been avoided, there was a lack of evidence as to causation. While this is a proper procedure for defending against opposing experts — trying to rebuke the expert's relevance — the defendants in this case were unsuccessful. The court explained the expert report must provide a "fair summary" of the expert's opinions regarding the applicable standard of care, how the care rendered by the defendant physician or healthcare provider breached the standard of care, and the causal relationship between the failure and the damages claimed. Here, the patient's expert satisfied these requirements, and the court afforded weight to the expert's opinion. Although the defendants in this case were unsuccessful, this case confirms that procedurally, challenging a patient's expert may prove worthwhile. If the expert's qualifications are questioned, the expert's opinions and harmful conclusions may be excluded. At a minimum, undermining an opposing expert can help bolster a care provider's own expert opinion, making it appear more reasonable and appropriate. ■

REFERENCE

Decided Aug. 25, 2020, in the First Court of Appeals of Texas, Case Number 01-19-00094-cv.