HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE SINCE 1979

INSIDE

RELIAS MEDIA

JULY 2019 Vol. 41, No. 7; p. 73-84

DOJ's New Guidance on Corporate Compliance Provides Valuable Tool for Risk Managers

The Criminal Division of the U.S. Department of Justice (DOJ) recently released a guidance document for white-collar prosecutors on the evaluation of corporate compliance programs, and it should be a valuable tool for risk managers.

The document updates a prior version issued by the division's Fraud Section in February 2017. DOJ issued a statement saying the new guidance "seeks to better harmonize the guidance with other department guidance and standards while providing additional context to the multifactor analysis of a company's compliance program." *(The updated guidance is available online at: https://bit.ly/2lEphmk.)*

The guidance signals the DOJ's commitment to corporate compliance programs, says former assistant U.S. attorney **Jason Mehta**, JD, now an attorney with the Bradley law firm in Tampa, FL.

> "ENFORCEMENT IS HERE TO STAY FOR THE LONG HAUL, AND THE MORE COMPANIES RECOGNIZE THAT, THE MORE THEY CAN SEE CORPORATE COMPLIANCE AS A CHANCE TO IMPROVE."

"While many would have thought that the government would be more lax in corporate enforcement under the Trump administration, this policy in some ways is more robust and more vibrant than in past administrations," he says. "Enforcement is here to stay for the long haul, and the more companies recognize that, the more they can see corporate compliance as a chance to improve

Financial Disclosure: Author **Greg Freeman**, Editor **Jill Drachenberg**, Editor **Jesse Saffron**, Editorial Group Manager **Leslie Coplin**, 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. ReliasMediaSupport@reliasmedia.com ReliasMedia.com

SUBSCRIPTION PRICES: USA, Print: 1 year (12 issues) with free CE nursing contact hours, $519. Add $19.99 for shipping & handling. Online only, single user: 1 year with free CE nursing contact hours, $469. Outside USA, add $30 per year, total prepaid in USA funds.

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 Learning 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: Jesse Saffron
EDITORIAL GROUP MANAGER: Leslie Coplin
ACCREDITATIONS MANAGER: Amy M. Johnson, MSN, RN, CPN

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

rather than as yet another hurdle to overcome."

Any time the government lays out its thinking and its metrics on how it evaluates compliance programs, risk managers should really be paying attention, Mehta says.

"This is the playbook of how the government is going to evaluate corporate compliance programs, the roadmap, and the things it cares about. Healthcare companies would be well-served by scrutinizing this guidance and making sure their own programs comport with it," he adds.

The guidance explains that companies need to tailor their corporate compliance programs to the risks facing the organization, Mehta says. Companies should identify their areas of high risk and low risk, apportioning their resources and efforts accordingly.

"Understanding that baseline expectation is really critical. It should force healthcare companies to think critically about their own companies, where they have vulnerabilities, and devote the corresponding resources there," Mehta says.

The guidance also makes clear that DOJ expects companies to police third parties they work with. "This really puts a burden on companies to understand who their partners, agents, and consultants are, and then to think about whether they are doing enough due diligence on these parties," he says. "That means understanding things like who the top referrers are, the top prescribers, and making sure that not just your own company is compliant but those third parties are, too."

The government also is focusing on how a compliance program is implemented and maintained — not just how it is initially formed, Mehta notes. Risk managers should make sure that executives in the company are demonstrating leadership with the compliance program, modeling proper behavior, and not tolerating compliance risks. Companies also must ensure that all employees are educated on the compliance program.

Plenty of Advice From DOJ

This recent guidance from the DOJ is another welcome prosecutorial focus on the importance of compliance programs, says **Gary Giampetruzzi**, JD, partner at the Paul Hastings law firm in New York City and vice chair of the firm's Life Sciences practice.

"It breaks the subject of programs down nicely from the design with the expected subcategories of coverage, to the effort at the implementation, and then the question of whether the program was effective in operation

EXECUTIVE SUMMARY

The Department of Justice (DOJ) issued new guidance on corporate compliance programs. Risk managers should use the guidance to tailor and optimize their compliance programs.

- The guidance provides specific questions to ask about your own program.
- DOJ expects companies to police the compliance of third parties.
- The guidance illustrates DOJ's expectation that effective compliance programs will evolve over time.

— the latter two core categories also including subcategories of coverage," Giampetruzzi says.

"While a document 19 pages or so in length cannot spell out all that could be spelled out on the broad topic of compliance programs, this one does offer enough to enable internal and external practitioners alike to confirm what might have been existing thinking — or, in some cases, redraw focus on topics that tend to fall out of focus for too many at times, like the subject of threshold risk assessments — which receives a fair amount of real estate — and relatively thorough treatment for what could be otherwise considered such an established topic."

There also are elements of the document that suggest a keener understanding today regarding the actual complexities associated with operationalizing compliance programs, which the document specifically calls out, Giampetruzzi says. The role of controls gatekeepers also receives what he calls an interesting and justifiable focus.

"The importance of the close cousin to the compliance control — the financial control — is very much present for those looking for it, and really needs to be considered by the compliance professionals more routinely focused on compliance policies and procedures," he says.

Giampetruzzi notes that there is even a good question nestled in the guidance regarding compliance resources: "Have there been times when requests for resources by compliance and control functions have been denied, and if so, on what grounds?"

"The operationalization of that Q&A itself should prove interesting within some companies," he says. "All in all, a pretty good effort by the DOJ on the subject of compliance."

More Detail Than Previous Guidance

Much of what is new in the guidance is the level of detail rather than a major shift in policy, says **Jason de Bretteville**, JD, shareholder and chair of the litigation department with the Stradling law firm in Newport Beach, CA. It addresses familiar topics including the role of the compliance function within the organization, the need for skilled internal investigators, the limits of outsourcing compliance functions, the relationship between risk assessment and program design, and the role of compliance in mergers and acquisitions transactions — all with a greater level of detail than what is provided in the existing guidance, he says.

It should be used to educate and secure support for the compliance function from directors and senior executives, and as a resource in assessing the adequacy of existing compliance efforts, de Bretteville says.

"The most fundamental aspect of the guidance is its focus on the need to perform and document a meaningful risk assessment as a predicate to designing a tailored 'fit for purpose' compliance program," de Bretteville says.

He cites these key points of emphasis in the guidance: the need to establish an autonomous and robust compliance function on par with other key business units; involve business stakeholders in designing a risk-based program; achieve demonstrable buy-in from middle and lower management; provide training that is tailored to each audience and includes real-world examples; incorporate both incentives for good behavior and consequences for breaches; conduct meaningful testing; and perform a root cause analysis in response to any breach and implement changes that address that root cause as part of remediation.

"For larger enterprises with mature compliance programs, the guidance provides a basis on which compliance officers can drive the organization to improve program design by undertaking meaningful assessment of the unique risks faced by healthcare organizations on a reiterative basis, and devote adequate resources to that program," de Bretteville says. "For smaller companies, the emphasis on risk assessment will help compliance officers advocate for and defend more focused and efficient compliance programs that target the greatest sources of risk to the specific organization."

Begin With Formal Risk Assessment

When evaluating whether a compliance program is well-designed, a critical step is to begin with a formal risk assessment, says **Anthony J. Phillips**, JD, principal with the McKool Smith law firm in Houston.

The risk assessment should focus on the risks and types of misconduct most likely to occur in the organization's line of service, particularly the most relevant regulatory structures and requirements. Compliance professionals should use the results of this risk assessment to guide the drafting of policies and procedures that appropriately address risk areas, and training programs for employees and important third parties such as agents, affiliates, and acquisition targets, he says. The assessment also should guide a communication plan to ensure the program's messaging is broadly delivered.

"It is best to benchmark one's program against peer organizations — both by lines of service and institutional size — and to update the risk assessment periodically, ensuring that one's program is keeping up with changing risks and compliance industry norms," Phillips says.

Once confident in the compliance program design, it is important to ensure that the program is implemented effectively, he says. Leadership must set the correct tone from the top of the organizational structure, and a culture of compliance must be integrated throughout the organization.

"These goals can be achieved by ensuring that the organization's compliance function is well-resourced and has sufficient autonomy to review, investigate, and remediate potentially noncompliant processes by supporting regular audits of high-risk areas, and by ensuring effective discipline in the event that actual misconduct is discovered," Phillips says. "In fact, organizations should proactively encourage inquiries to the compliance office and reporting of potential misconduct. It is equally important to guarantee freedom from retaliation and protection for good-faith reporters and witnesses cooperating with an investigation."

The effective compliance program will incorporate real-world compliance issues faced by the organization into employee and third-party training and certification programs, Phillips says.

An organization also has to ensure that the compliance program is working, Phillips says. Of significant importance is broad dissemination of compliance program results in an effort to ensure a thorough understanding of the role of compliance in the organization, he says. An effective compliance program might include regular messaging from senior management of compliance "saves" as well as anonymized discipline for policy violations.

"It is also important to ensure that compliance reports are promptly and effectively investigated, including root cause analysis, any necessary training or certification of actors involved, and documented accountability for mistakes or misconduct, up to and including termination, where appropriate," he says. "A compliance program that is working properly will learn from trends in compliance reporting, the findings of investigations, and any necessary remediation efforts to continuously improve the program."

Phillips adds another point that is not in the guidance but that is particularly useful for compliance professionals: Proactively involve other administrative functions in your compliance program. The legal department, human resources, internal audit, and corporate security all are natural allies of the compliance department, he says. A compliance professional can create powerful synergies with these allies that strengthen the program's design, improve implementation, and ensure that the program is actually working, he suggests.

No Rigid Formula for Prosecution

It is not clear how the DOJ will use the 2019 guidance going forward, says **Kathy Butler**, JD, an officer and leader of the Healthcare Practice Group at Greensfelder, Hemker & Gale in St. Louis. Many of the concepts that are explained in more detail in the 2019 guidance have been used by prosecutors in the past when making enforcement decisions, she notes.

"The 2019 guidance itself notes that there is no rigid formula to assess the effectiveness of a corporate compliance program, and the sample topics and questions are not designed to be a checklist or a formula," Butler says. "Each organization's compliance program will be different based on risk profiles and resources, and each will be evaluated by the DOJ in the specific context of a criminal investigation. The 2019 guidance sets forth the common questions prosecutors will take into consideration when evaluating a corporate compliance program during an enforcement action, but it is guidance — not law or regulation —

and not all of the guidance will apply to every corporation."

However, Butler says, publishing the 2019 guidance effectively puts healthcare providers on notice of what prosecutors will be looking at when they evaluate compliance programs, including design and operation with respect to training, investigations, and management. The framework of the guidance gives providers a resource to proactively assess their compliance programs based on relevant portions of the guidance, and if necessary, make changes to improve their polices and processes, she says.

"Providers who use the 2019 guidance as a resource to improve their corporate compliance programs may reduce the risk of compliance failures that may lead to investigation or prosecution. Or, if the provider should become the subject of an investigation, demonstrate the provider's efforts to maintain an effective compliance program," Butler says. "Healthcare risk managers should read the 2019 compliance guidance carefully, and use the questions in the document that are relevant to that provider to evaluate the current status of the provider's corporate compliance program."

The DOJ understands that corporate compliance programs will differ based on the provider's risk profile and resources, Butler says, but in any enforcement action, DOJ will expect prosecutors to ask the three fundamental questions with respect to program design, implementation, and effectiveness.

"The 2019 compliance guidance focuses on the compliance program from top to bottom, so getting senior and middle managers involved in the compliance process is an important part of the evaluation," Butler says. ■

SOURCES

- **Jason de Bretteville**, JD, Shareholder, Stradling, Newport Beach, CA. Phone: (949) 725-4094. Email: jdebretteville@sycr.com.
- **Kathy Butler**, JD, Officer, Greensfelder, Hemker & Gale, St. Louis. Phone: (314) 516-2661. Email: khb@greensfelder.com.
- **Gary Giampetruzzi**, JD, Partner, Paul Hastings, New York City. Phone: (212) 318-6417. Email: garygiampetruzzi@paulhastings.com.
- **Jason Mehta**, JD, Bradley, Tampa, FL. Phone: (813) 559-5532. Email: jmehta@bradley.com.
- **Anthony J. Phillips**, JD, Principal, McKool Smith, Houston. Phone: (713) 485-7309. Email: aphillips@mckoolsmith.com.

Time Component Is One of Major Takeaways in Guidance

The U.S. Department of Justice (DOJ) guidance on corporate compliance includes an important time component instructing prosecutors to consider the effectiveness of a compliance program not only when misconduct occurred, but when making charging decisions and upon resolving a case, notes **Jennifer L. Evans**, JD, office managing partner with the Polsinelli law firm in Denver.

The guidance illustrates DOJ's expectation that effective compliance programs will evolve over time based on the legal risks in a company's general business operations and during transactions and business change when risks may increase, she says.

Evans notes that the DOJ's Criminal Division instructs prosecutors to ask three questions when evaluating a corporate compliance program:

- Is the corporation's compliance program well-designed?
- Is the compliance program being implemented effectively?
- Does the compliance program work in practice?

These elements are not new, she notes, but the guidance should help companies evaluate their compliance effectiveness. Evans provides the following summary of major takeaways from the new guidance:

- **Risk assessments are critical.** The government expects an effective compliance program to uniquely respond to compliance risks in a company's operations. Not all similar companies will have the same risk profile, and risk assessments should occur on regular basis.

Four factors are of particular importance. Increased risk when starting a new line of business is a primary concern, along with mergers and acquisitions (M&A). With M&A, companies must consider the compliance of target companies with a plan to fix if needed. Working with third-party managers and vendors also is important. Arrangements must be carefully structured and have significant compliance oversight to protect a company from permitting or encouraging a violation of law through someone else. Risk assessments should be completed for new activities and repeated on a regular basis for ongoing business

lines, with the risk assessments changing over time based on results.

• **Measure results, and respond.** The government expects effective compliance programs to respond to risk assessments and changed business environments by testing and measuring results. Routine evaluations should lead to measurable results of compliance with company requirements and the law. Without the ability to report identification, investigation, and remediation of compliance issues, a company cannot adjust its compliance program to address its key risks, and the government will not view the compliance program as effective.

• **Effective compliance programs are dynamic.** The government expects an effective compliance program to change over time in response to changed risks, business practices, and markets. In addition to regularly scheduled reports, audits, and risk assessments, the compliance program should respond and fine-tune requirements based on those inputs and external changes in the business environment. When budgeting time and economic resources for compliance, there should be capacity for both ongoing oversight and unexpected issues that may arise. An effective compliance program today, unchanged, will not be an effective compliance plan tomorrow.

William H. Maruca, JD, partner with the law firm of Fox Rothschild in Pittsburgh, also notes that a well-designed program should cover risk assessment, policies and procedures, training and communications, confidential reporting structure and investigation process, third-party management, and M&A.

A well-designed compliance program should apply risk-based due diligence to its third-party relationships, Maruca says. That should include risk-based and integrated processes, appropriate controls, management of relationships, and real actions and consequences. ■

SOURCES

- Jennifer L. Evans, JD, Office Managing Partner, Polsinelli, Denver. Phone: (303) 583-8211. Email: jevans@polsinelli.com.
- William H. Maruca, JD, Partner, Fox Rothschild, Pittsburgh. Phone: (412) 394-5575. Email: wmaruca@foxrothschild.com.

Supreme Court Extends False Claims Act Limit to 10 Years for Most Cases

The U.S. Supreme Court recently expanded the statute of limitations period for nonintervened whistleblower False Claims Act (FCA) cases from six to 10 years.

The decision involving Cochise Consultancy addressed which of two statutes of limitation in the False Claims Act applies in the event a relator brings an action but the government has not intervened, explains **Eric H. Cottrell**, JD, partner with the Parker Poe law firm in Charlotte, NC. There was a dispute among different circuits, he says.

The first statute of limitations sets a limit of six years after the violation, but a second sets a limit of three years after the facts were known or reasonably should have been known by government officials and in no case later than 10 years after the violation, Cottrell says. The defendants in the case argued that the second and longer statute of limitations applies only when the government intervenes in the case. *(The Supreme Court ruling is available online at: https://bit.ly/2IvI5xw.)*

Act Intended to Shift Limits

"Their argument was fairly interesting and seems fairly reasonable on its face, arguing that the government's knowledge should really be an issue only when it is party to the case," Cottrell explains. "The court's ruling is that the statute's meaning is just what it says. The court did not delve deep into the policy reasoning underlying the statute, and just said the statute speaks for itself."

The ruling determined that the False Claims Act was purposefully written to move cases from one period of limitation to another when a U.S. government official is informed of the impending action. The court also addressed the question of who constitutes a government official charged with acting in an FCA case, again sticking with the plain language of the statute, Cottrell explains.

"The main takeaway here is that whatever errors in compliance you make, they are likely to live with you a lot longer than they used to," Cottrell says. "That is particularly true in the 4th and 10th circuits, which had both adopted the first interpretation of the statute limitations, saying the longer limit

did not apply when the government did not intervene."

The government doesn't intervene in the vast majority of FCA cases, so in those circuits, the statute of limitations was six years after the violation, Cottrell explains.

"Now, defendants in those cases have to reckon with the fact that the statute of limitations is going to be extended an additional four years," he says. "That is not only going to affect the number of cases brought, but it is also going to increase the damages calculations. That is going to have a pretty big impact."

The Supreme Court ruled unanimously that the language of the False Claims Act was unambiguous and that it meant that the statute of limitations extension applied in cases brought by whistleblowers where the government did not intervene, notes **Jesse Witten**, JD, partner with Drinker Biddle in Washington, DC, and a former deputy associate attorney general in the U.S. Department of Justice.

"In my opinion, the statute was very unclear. It is certainly possible to interpret the plain language of the statute in the way that that Supreme Court did, but it is also possible to interpret the statutory language to reach the opposite conclusion that the statute of limitations extension is not available in nonintervened *qui tam* cases being litigated by the whistleblower," Witten says. "In fact, many lower courts interpreted the statute to mean the opposite of how the Supreme Court ruled."

Under this ruling, a whistleblower could have waited 10 years to file the *qui tam* action, but so long as the Department of Justice did not know of the material facts more than three years before it was filed, the statute of limitations has not expired, Witten explains.

"The result of this decision is that relators will be able to bring older cases than they could previously. That means that some cases that would have been dismissed as untimely will now survive," Witten says.

"More importantly, it means that defendants will face larger potential damages and penalties for many cases. Had the case come out the other way, a healthcare provider would only be liable for potential damages and penalties for claims that were submitted within six years of the filing of the *qui tam* lawsuit, but now can be liable for claims submitted within 10 years of the filing — four more years' worth of damages and penalties."

One question is whether this case will inspire more old *qui tam* lawsuits to be filed, Witten says. Since every *qui tam* whistleblower hopes that the government will intervene, and since the statute of limitations extension clearly applies to intervened cases, Witten says, there is little motivation for someone to now file a case if they would not have previously.

"In addition, for cases brought against defendants that do business in multiple jurisdictions, even before *Cochise*, many whistleblowers could have strategically selected one of those venues for their *qui tam* lawsuit where the lower court had already held that the statute of limitations extension applies to intervened cases," Witten says.

One issue that healthcare organizations must think about is when they discover Medicare or Medicaid overpayments that stretch back longer than six years or that occurred more than six years ago, Witten says. Under the Affordable Care Act, healthcare providers must refund and disclose Medicare and Medicaid overpayments within 60 days of identifying the overpayment, or else face FCA exposure for the failure to refund. The Centers for Medicare and Medicaid Services (CMS) has advised in its overpayment regulation that the lookback period for these overpayments is six years, Witten notes.

"I do not think that the *Cochise* decision should alter whatever conclusion healthcare organizations have already reached about what to do with overpayments that occurred between six and 10 years ago that they have identified. It remains reasonable to rely on the CMS overpayment guidance," he says. "In addition, even before *Cochise*, the government had the authority to file suits with allegations dating back 10 years, depending on when the government learned of material facts."

From a practical standpoint, relators may be incentivized to wait years to report conduct in order to increase potential recovery on their claims, says **Damaris L. Medina**, JD, shareholder with the Buchalter law firm in Los Angeles.

Whistleblower attorneys may also be mistakenly emboldened in arguing that they have more leverage than before to negotiate a settlement when the government decides not to intervene in a case, basing their argument on the court's comment that a False Claims case remains largely unchanged — except for the removal of a party — when the government doesn't intervene, Medina says.

"All of these potential consequences point toward hospitals, hospital systems, physician groups, and all other healthcare providers increasing their compliance efforts. Specifically, providers should make sure that they create and/or maintain a culture where any compliance issues are, and can be, reported immediately without fear of retaliation," Medina

says. "In addition, once reported, providers must make sure that any compliance issues are investigated and addressed as quickly and thoroughly as possible to decrease the potential liability associated with any continued conduct under the newly interpreted limitations period."

Providers also may consider increasing the frequency of their auditing procedures in order to identify any potential issues in a timely manner, and may contemplate availing themselves of self-disclosure protocols where appropriate in an effort to mitigate additional risk, Medina suggests.

Emphasize Corporate Compliance

Continuing, implementing, or expanding a strong compliance program is the best defense against possible FCA suits, says **Kevin P. Mulry**, JD, partner with the Farrell Fritz law firm in Uniondale, NY. Companies also will want to consider whether their document retention programs should be revised to provide for a longer retention period so that relevant documents will be available to defend FCA allegations that could reach back for a decade or more.

The healthcare industry perennially accounts for the majority of new FCA cases and recoveries, says **D. Jacques Smith**, JD, complex litigation practice leader with the Arent Fox law firm in Washington, DC. In fiscal year 2018 alone, the DOJ reported that more than $2.5 billion of the nearly $2.9 billion in total FCA recoveries involved the healthcare industry, Smith notes.

In light of *Cochise*, even when a healthcare company discovers a potential FCA violation that is several years old, it must take the potential violation seriously, investigate as necessary, and in some circumstances consider a self-disclosure to the Health and Human Services Office of Inspector General or the Department of Justice, with the assistance of experienced FCA counsel, Smith says.

"And if a company or individual receives a subpoena or Civil Investigative Demand from a government authority, the company or individual should promptly retain experienced FCA counsel to handle the response and related strategy," Smith says. "This could be an early indication that a relator has filed a sealed FCA complaint against the company, and that the government is investigating the allegations to decide whether to intervene and take other action."

Healthcare fraud cases account for nearly 50% of the lawsuits initiated under the FCA, notes **Brian F. McEvoy**, JD, chair of government investigations with the Polsinelli law firm in Atlanta. Nearly every year, the number of FCA cases increases, and the amount of money recouped by the government from verdicts and settlements from healthcare and other entities has reached $3 billion annually. This doesn't include the many millions of dollars that whistleblowers recover as part of their reward under the law for bringing suit on behalf of the government, he says.

Since the government declines to intervene in nearly 85% of FCA *qui tam* cases, the court's ruling in *Cochise* effectively extends the statute of limitations for a vast majority of relators for an additional four years, McEvoy says.

"The increased statute of limitations may create new burdens for healthcare entities defending FCA claims, as allegations and subsequent discovery obligations may extend over dozens of years," McEvoy says. "It is also worth noting that the unanimous opinion, authored by Justice Thomas, suggested that nonintervened *qui tam* [cases] should be allowed the same deference as those the government intervenes in."

The court observed that "If the government intervenes, the civil action remains the same — it simply has one additional party." The *Cochise* decision also allows the government to pursue other avenues of discovery, McEvoy says.

"Indeed, a relator intending to use the 10-year limitations period must file the complaint within three years of when 'facts material to the right of action are known or reasonably should have been known' by 'the official of the United States charged with responsibility to act in the circumstances,'" McEvoy explains. "Justice Thomas' opinion opens the door to defendants issuing further discovery to help determine when the government knew or should have known of the material facts."

The *Cochise* ruling is likely to lead to an increase in FCA litigation and, with it, many opportunities to analyze how defendants plan to seek discovery from the federal government, McEvoy says.

"While the court's opinion has made it easier for relators to pursue FCA claims, it does not change the strategy of healthcare providers looking to prevent and defend against FCA actions," he says. "A robust and thoughtful regulatory compliance program combined with counsel experienced with FCA claims are essential to limiting potential exposure to future FCA actions." ■

SOURCES

- **Eric H. Cottrell**, JD, Partner, Parker Poe, Charlotte, NC. Phone: (704) 335-9850. Email: ericcottrell@parkerpoe.com.

- **Brian F. McEvoy**, JD, Chair of Government Investigations, Polsinelli, Atlanta. Phone: (404) 253-6021.
- **Damaris L. Medina**, JD, Shareholder, Buchalter, Los Angeles. Phone: (213) 81-5224. Email: dmedina@buchalter.com.
- **Kevin P. Mulry**, JD, Partner, Farrell Fritz, Uniondale, NY. Phone: (516) 227-0620. Email: kmulry@farrellfritz.com.
- **D. Jacques Smith**, JD, Complex Litigation Practice Leader, Arent Fox, Washington, DC. Phone: (202) 857-6154. Email: jacques.smith@arentfox.com.
- **Jesse Witten**, JD, Partner, Drinker Biddle, Washington, DC. Phone: (202) 230-5146. Email: jesse.witten@dbr.com.

LabCorp and Quest Breaches Show Vulnerability of Data

Data breaches recently reported by two major laboratory testing companies illustrate the vulnerability of protected health information provided to vendors.

Quest Diagnostics reported that 11.9 million customers' medical and financial information may have been exposed due to a breach at one of its billing collections vendors, American Medical Collection Agency (AMCA). LabCorp reported the next day that 7.7 million of its patient accounts at AMCA also may have been compromised.

All sectors are seeing an increase in breaches due to third-party service providers, business associates/partners, and even commercial off-the-shelf products compromised during manufacture, says **Jeff Roth**, southeast regional director at NCC Group, a cybersecurity and risk mitigation company based in the United Kingdom. Some of the top reasons include the increased use of managed services without adequate qualification and validation of these third parties' security posture, and not incorporating the organization's cybersecurity requirements (along with referenced responsibility matrices) within the service provider, business partner, and subcontractor contracts, he says.

There also is a failure of organizations to fully integrate the supply chain (service providers, business partners, and subcontractors) within the organization's continuous monitoring, vulnerability management, incident response programs, and processes, he says.

Roth says the following factors are critical to success in addressing these concerns:

• The board of directors'/trustees' direction to senior management that supply chain security is a priority and a distinct part of the cybersecurity goals and objectives;

• Assurance that adequate resources are allocated as actual budget line items to develop, implement, and maintain an ongoing and relevant supply chain cybersecurity program;

• Integration of the supply chain cybersecurity processes through the acquisition life cycle across the organization;

• Regular, independent validation that the supply chain cybersecurity program and respective processes remain in place, operating effectively and adapting to changes in threat, geopolitical, and business environments.

"Without adequate contract requirements for supply chain cybersecurity, organizations will be primarily responsible for breach disclosure. There should be one entity in charge of disclosure to all stakeholders, customers, public, and regulatory agencies," Roth says. "And service providers, subcontractors, and business partners need to be incorporated in the incident response processes so the organization maintains consistency in all disclosures. The primary reason for this is to prevent inaccurate or even misleading releases of information or release of information that could hamper criminal and civil investigations."

The breaches are a further sign that supply-chain attacks are increasingly popular with criminals, says **Stuart Reed**, vice president at Nominet, a cybersecurity company based in the United Kingdom.

"This should be taken into account during contractual negotiations. Never assume a supplier is acting responsibly," Reed says. "Seek proof and build key performance indicators, reinforced by regular audits and tests to ensure suppliers are upholding their obligations. Protection of data throughout the supply chain is a collective responsibility, and any weak point presents a target of opportunity for an attacker."

"This is a collaborative process and one that relies on getting risk management and cybersecurity embedded into the partner relationship early on," Reed adds. "As digital transformation grows and swells the attack surface

ever wider, this should become something that is baked into all supplier contracts as matter of routine."

Any organization that used AMCA's website during the period when it was compromised also could become a victim of data leakage, notes **Leigh-Anne Galloway**, cybersecurity resilience lead at Positive Technologies, a cybersecurity company in Boston.

"There are several methods an attacker can use to steal data entered on websites, as was the case in these breaches. Recently, we've seen JS-sniffer attacks become popular among hackers. This malware infiltrates a website and intercepts information entered," she explains. "Leaks also often occur as a result of attacks with SQL injection, which allow criminals to get all the information from the site's databases. And there are frequent cases of leaks caused by administration errors, when access to a database is not at all limited and anyone who connects to them can access the data."

In order to avoid such third-party breaches, organizations should clearly state their requirements on information security, she says. If the third-party company cannot guarantee the fulfillment of those requirements in relation to the transmitted data, it is worth contacting another, Galloways says.

"Organizations should also initiate an audit of third-party entities they plan to do business with in order to make sure data is processed and stored safely before signing agreements," she says. "Based on the audit results, the company can decide whether to move forward with business." ■

SOURCES

- **Leigh-Anne Galloway**, Cybersecurity Resilience Lead, Positive Technologies, Boston. Phone: (857) 208-7273.
- **Stuart Reed**, Vice President, Nominet, United Kingdom. Phone: (202) 821-4256.
- **Jeff Roth**, Southeast Regional Director, NCC Group, United Kingdom. Phone: (800) 813-3523.

Leapfrog Sees Improvements in Patient Safety

Poor hospital performance on 16 patient safety measures causes more than 161,000 deaths annually, according to a recent report from the Leapfrog Group and Johns Hopkins — but that is a decrease from 2016 figures.

The Spring 2019 Leapfrog Hospital Safety Grades looks at deaths due to errors, accidents, injuries, and infections, comparing them to the hospitals' A through F Leapfrog scores.

There was a 92% greater risk of avoidable death at D and F hospitals than at A hospitals, the report says. The analysis included 2,600 hospitals.

Compared to A hospitals, there was an 88% greater risk of avoidable death at C hospitals and a 35% greater risk at B hospitals.

"Even A hospitals are not perfectly safe, but researchers found they are getting safer," according to the report. "If all hospitals had an avoidable death rate equivalent to A hospitals, 50,000 lives would have been saved, vs. 33,000 lives that would have been saved by A-level performance in 2016."

Current data suggest 160,000 lives are lost each year to avoidable medical errors, Leapfrog says. The 2016 report estimated 205,000 avoidable deaths annually. *(The current report is available online at: https://bit.ly/2WNecia.)*

Leapfrog also recently released its 2019 Maternity Care Report, which found that only 20% of the reporting hospitals are fully in compliance with Leapfrog's standards on cesarean sections, early elective delivery, and episiotomy rates. *(The report is available online at: https://bit.ly/2W18gB2.)*

The report on lives lost shows clear progress in improving patient safety, says **Leah Binder**, CEO of The Leapfrog Group in Washington, DC.

"Typically, when we talk about patient safety, we don't talk about improvement because it seems like an intractable problem that never goes away. Finally, we have very good news," Binder says. "Forty-five thousand people not dying each year is a lot of people. This is encouraging, and we should at least take one pat on the back for American hospitals that they are on the right track for addressing safety."

But the praise is limited, Binder says, because 160,000 lives lost annually is still a huge problem.

"We still have a long way to go before we can pop the champagne, but we're on the right track, and it has been a very long time since any of us could say anything positive about our effectiveness in addressing patient safety," Binder says.

Binder encourages risk managers to look at whether their hospitals are declining to report some of the data included in the report. Some hospitals are not transparent about data that might not be flattering, so risk managers should consider that a red flag and address the underlying issues, she says.

The Leapfrog report is encouraging, suggesting that hospitals are making progress on reducing patient harm, and that efforts have resulted in an overall reduction in lives lost, says **Lisa Simm**, RD, MBA, CPHQ, CPPS, CPHRM, FASHRM, manager of risk management with Coverys, a liability insurer based in Boston.

Simm notes that healthcare executives have openly expressed some justifiable criticism of the Leapfrog Safety Score methodology, including concerns regarding the validity of the self-assessment/self-reporting nature of the survey, lack of adequate severity adjustment for all outcome measures, limitations in the use of payment codes to collect clinical quality data, variation in data collection time periods between measures taken from January 2015 to March 2018, and questions as to the meaningful nature of benchmarking hospitals of all sizes, serving very different populations — especially when not all hospitals can participate in all the outcome measures.

However, the Armstrong Institute of Patient Safety and Quality of Johns Hopkins Medicine, understanding these limitations, joined forces with Leapfrog in an effort to test solutions. Simm says they are using a scientific approach in an effort to advance patient safety and quality and specifically achieve meaningful ways to provide purchasers, patients, and families with hospital quality of care information to help them determine value.

"This report should serve to substantiate patient safety achievements and the need for improvement in both patient safety and our ability to measure quality of care and patient safety," Simm says. "This report is a reminder that the purchasers of insurance and their patients are certainly interested in making informed healthcare purchasing decisions that consider the quality of healthcare provided in hospital care."

Quality and risk management professionals should remember that the ability to measure quality and predict risk is in its infancy in healthcare, Simm says.

"The estimated mortality rate of patient safety events in this report has not taken into account a severity adjustment or comorbid conditions for each outcome measure in a given hospital, ICU, or obstetrical unit, and a hospital can receive a safety score of A without reporting values on all their outcome measures," she says. "The report is using the best of what we have available."

Quality improvement and risk management professionals and clinicians should be involved with suggesting and developing the best measures to evaluate hospital care, Simm says.

"This is not easy, but they are the experts who are best positioned to do so. They should be involved at the national or regional level with their professional societies and expert measure development coalitions, and they should share their expert provider input on the most valid and reliable measures used for benchmarking," she says.

This report also is a reminder of the leadership role risk management and quality improvement professionals have in prioritizing and driving improvement within their own organizations, Simm says.

"This report, like other studies, supports the premise that patient harm is likely underreported and underestimated and that risk management and quality improvement professionals need to work together to develop more robust adverse event identification systems and take that one step further by developing early warning systems that can help prevent harm from occurring," she says. "There is a need for improved outcome measurement and increased process measures that align with outcomes. The signals provided by this report need to be considered with all the other quality and patient safety signals an organization is receiving."

The report also signals the need for further development in outcomes measurement that looks at the entire community health system and not just the hospital in isolation. Hospitalization can be a factor of the health of the population and whether appropriate supports are available in the community for a given population, she notes.

Benchmarking with best-in-class hospitals can be effective in formulating improvement in operations and processes, Simm notes.

"Appropriate benchmarking cohorts make any benchmarking data more meaningful. Not all patients are alike, and our hospitals service clients with differing complexities in clinical need, comorbidities, social determinants, and community resources," she says. "Data transparency and the need to benchmark will continue to play a role in performance improvement and is useful to purchasers and their patients. Hospitals will want to select the most comparable organizations with target levels of performance they are looking to achieve." ■

SOURCES

- **Leah Binder**, CEO, The Leapfrog Group, Washington, DC. Phone: (202) 292-6713.
- **Lisa Simm**, RD, MBA, CPHQ, CPPS, CPHRM, FASHRM, Manager, Risk Management, Coverys, Boston. Phone: (800) 225-6168.

HEALTHCARE RISK MANAGEMENT™

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 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 e-mailed to you.

CME/CE QUESTIONS

1. **What does Jason Mehta, JD, say is one key point from the guidance on corporate compliance from the DOJ?**

   a. Companies need to tailor their corporate compliance programs to the risks facing the organization.
   b. The DOJ is relaxing its expectations for corporate compliance.
   c. The DOJ expects companies to follow one corporate compliance model outlined by the government.
   d. Companies need to tailor their corporate compliance programs to a set of specified risks in that industry from the DOJ.

2. **What is the effect of the U.S. Supreme Court case involving Cochise Consultancy?**

   a. The ruling expanded the statute of limitations period for nonintervened whistleblower False Claims Act cases from six to 10 years.
   b. The ruling limited the statute of limitations period for nonintervened whistleblower False Claims Act cases to six years.
   c. The ruling determined that the intervention of the government has no bearing on the statute of limitations.
   d. The ruling identified which specific government officials must be notified for the statute of limitations to be extended.

3. **In what percentage of False Claims Act lawsuits does the government decline to intervene?**

   a. 25%
   b. 45%
   c. 65%
   d. 85%

4. **According to a recent report from the Leapfrog Group and Johns Hopkins, what was the increased risk of avoidable death at D and F hospitals than at A hospitals?**

   a. 12%
   b. 32%
   c. 62%
   d. 92%

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

Hospital and Physicians Liable in Case of Woman Who Died Hours After Giving Birth

*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 jury found a hospital and team of physicians negligent for a patient's death shortly after giving birth, caused by significant blood loss due to a condition known by her physicians.

The condition created a high risk during delivery and should have been planned for accordingly to minimize the chances of life-threatening complications. However, the physicians who had followed the woman throughout the pregnancy and who were aware of the potential life-threatening complications failed to adequately prepare a plan for the scheduled cesarean section.

The patient's surviving husband filed a lawsuit on behalf of himself and their four children, alleging that the physicians and hospital's actions constituted medical malpractice. The jury agreed and awarded the patient's family a total of $24.5 million.

Background: From the initial stages of her pregnancy, the patient, a 34-year-old woman, was known to have a condition known as placenta previa and suspected to have placenta accreta. Placenta previa is a condition where the placenta attaches low in the uterus and can completely cover the cervix. Placenta accreta is a condition where the placenta attaches too deep into the uterine wall, which can lead to severe and uncontrolled bleeding during delivery. Both conditions are potentially life-threatening, requiring extreme caution and heightened attention. Patients suffering from either condition must be monitored closely throughout the pregnancy, and routine delivery practices should be adjusted to ensure that in the case of severe bleeding, physicians and staff are ready to immediately intervene.

THE PATIENT CLAIMED THAT THE PHYSICIANS AND HOSPITAL DID NOT ADEQUATELY PREPARE FOR THE POTENTIAL COMPLICATIONS CAUSED BY THE CONDITION.

The patient's physicians, who subsequently performed the cesarean section, were aware of the conditions affecting the woman during the early stages of her pregnancy and prenatal care. However, the patient claimed that the physicians and hospital did not adequately prepare for the potential complications caused by the condition.

On July 21, 2015, the patient entered the hospital for the scheduled cesarean section. The procedure was scheduled to take place at 10 a.m. but was delayed over 14 hours. The procedure finally took place at midnight on July 22 and was not performed on an emergency basis. During the procedure, the patient's placenta accreta caused substantial bleeding: The patient lost approximately 10 liters of blood and went into cardiogenic and pulmonary shock associated with severe hypoxia.

Moments after delivery, the patient was put on full ventilator support and a selective embolization of the left uterine artery was performed. The patient was transported to an operating room in an attempt to control the bleeding through an exploratory surgery. Despite these efforts, the patient was pronounced dead a few hours later as a result of multiorgan failure from hemorrhagic shock. Examinations confirmed that the low cervical cesarean section and placenta accreta caused the massive bleeding.

The patient's husband filed suit against the hospital and the treating physicians on behalf of himself and their four minor children. The complaint sought compensation for each individual's loss of support and services, and mental pain and suffering. The jury agreed that the hospital and physicians failed to provide care within the applicable standard, and awarded $3.7 million to the patient's husband, $4.9 million to each of the three eldest children, and $6.1 million to the youngest child, for a total award of $24.5 million.

What this means to you: The primary lesson in this case is for physicians and care providers to take into account a patient's specific medical history and medical conditions when determining the proper level of care and appropriate treatment for the patient. If a healthcare provider is aware of a relevant condition that may affect the course of treatment, then it may constitute medical malpractice to disregard that condition and otherwise proceed normally. In this case, the patient's surviving family successfully argued that the physicians were aware of her two existing medical conditions, that those conditions posed a threat, and that the physicians did not take the conditions into account when planning and treating the patient.

These conditions are not novel. They are well-known and well-researched, as they relate to a nationwide problem of maternal mortality, which has been consistently increasing since the 1970s and has placed the country's healthcare system under scrutiny. Placenta previa is a serious condition that can be seen on routine ultrasounds. Once that diagnosis is confirmed by a physician or radiologist, a vaginal delivery cannot take place safely in most cases and physicians must inform their patients that a cesarean delivery is the safest option. Placenta accreta, though less common, is a far more dangerous condition that usually requires not only delivery via cesarean section, but removal of the entire uterus via a hysterectomy as well due to the uterine tissue in the area of the accreta. This can present an emotional decision for a woman to make, especially if she was planning to have additional children. Physicians must allow a patient time to process the information about her condition and be well informed about what to expect.

Another important lesson from this case is that physicians and care providers must recognize when circumstances exist or change such that emergent action and care are required. In this case, the physicians delayed and performed a standard cesarean section without the additional care and security offered by emergency precautions and procedures. During delivery, if contractions are noted on the fetal monitor, the staff must proceed with the delivery on an emergent basis. Intravenous medications to stop any contractions should be given. An obstetrical hemorrhage should be anticipated during and after delivery for both conditions, and a sufficient supply of red cells, plasma, and other blood products must be available for immediate transfusion. The patient should be transferred to a high acuity postpartum unit with emergency equipment readily available and a well-trained staff with a low nurse/patient ratio.

As successfully argued by the patient's surviving family, the injuries that led to the death of the 34-year-old mother of four could have been prevented with adequate medical attention and preparation. Instead, after an initial diagnosis, the physicians failed to prepare and follow up with additional testing — which ultimately led to devastating consequences.

In particular, the patient's family alleged that following the initial visit, where placenta previa was diagnosed and where placenta accreta was suspected, physicians should have followed up with additional testing to confirm the diagnosis and should have monitored the pregnancy with increased attention, closely assessing the risks associated with delivery and changing the necessary circumstances of the delivery as needed. Specifically, physicians should have followed recommendations and performed a transvaginal ultrasound and obtained an MRI to confirm whether placenta accreta was present. Additionally, given the two conditions, the physicians should have performed a hysterectomy prior to the onset of uncontrolled bleeding. In fact, while a hysterectomy was performed on the patient during the surgery, the timing was not sufficiently prompt, and this delayed intervention caused the patient's extreme blood loss.

When presented with these facts and the applicable standards of care, the jury found the that the physicians were negligent and breached the required standard of care by planning to perform a routine procedure without taking into account the specific factors that created life-threatening risks for the patient. The follow-up procedures should have been performed at the time the condition was first suspected. Furthermore, the delivery and possible complications should have been planned for and the possibility of a hysterectomy in order to preventively control internal bleeding should have been taken into account.

The complaint also raised claims against the hospital where the patient received her care. These claims were brought under theories of agency and vicarious liability and alleged that the hospital should be held liable for the negligence of its employees or agents

who were acting within the scope of their employment or agency at the time of the incidents. Employer hospitals often are attributed such derivative liability as a result of the actions of their agents and employees.

Finally, a procedural, legal issue can be learned from this case as well: Prior to trial, the defendant physicians and hospitals conceded that their actions constituted malpractice, and admitted liability. Such an admission can serve multiple functions in the absence of a complete settlement between the parties, including by making the defendant care providers appear reasonable to a jury by acknowledging their mistakes and accepting responsibility. Additionally, this process greatly expedites any trial, which reduces the amount of time, effort, and attorneys' fees that must be spent in a futile attempt to defend a hopeless case. Considerations regarding stipulations concerning liability must be carefully weighed by care providers and their counsel, but may prove to be useful in litigation. ■

REFERENCE

Decided on April 18, 2018, Florida State Court, Case No. CACE18001011.

Patient Who Sustained Permanent Brain Damage After Asthma Attack Awarded $110 Million

News: A 48-year-old woman suffered an asthma attack while a patient at a hospital. Increased carbon dioxide in her body from the attack led to swelling in the patient's brain, and physicians failed to promptly treat the significant condition. The patient alleged that she should have been transferred to a facility with more advanced instruments and treatments, but such actions were not taken.

As a result, the patient suffered brain damage and permanent debilitating injuries, including lifelong speech and motor deficiencies resulting in permanent confinement to a wheelchair. She requires round-the-clock assistance, which she receives from her long-term life partner. Following trial, a jury agreed that the hospital's and physicians' actions constituted medical malpractice and awarded the plaintiff $110 million.

Background: In December 2010, a 48-year-old grandmother suffered a life-threatening asthma attack while she was a patient at a hospital. As the patient's asthma attack worsened, carbon dioxide buildup in her brain led to swelling. Given such circumstances, time is of the essence and so-called "salvage" treatments must be performed to prevent the patient from sustaining permanent injuries or death. In particular, when the condition is caused by elevated carbon dioxide levels, procedures must be implemented to rapidly increase the amount of oxygen entering the patient's bloodstream. Without prompt action and timely increase of oxygen levels, hypoxia will develop and lead to brain injuries. Other organs also may be damaged due to the fact that the bodily tissues are not receiving enough oxygen to function correctly. The hospital that had the patient in its care addressed the worsening condition by performing a treatment known as inhalation anesthesia, which is not as effective as other treatments.

However, this hospital did not have the necessary technology to perform extracorporeal membrane oxygenation (ECMO) or high-frequency oscillatory ventilation (HFOV). While this hospital did not have the capabilities, nearby facilities did. These treatments would have made a significant difference in how the patient's condition advanced and developed. Even as her condition worsened, the hospital and physicians did not consider the possibility of transferring her to a more advanced facility. Instead, the patient was moved to the "dark side" of the hospital's ICU, where her condition continued to worsen and the brain swelling caused permanent damage to her speech and motor functions, and confinement to a wheelchair.

In total, the patient spent 328 days in the hospital and nursing facilities before being able to return home. As a result of the patient's brain damage, she requires permanent assistance and medical care, which she receives from her long-term life partner.

Following her substantial injuries, the patient brought suit against the hospital and four individual defendant physicians who oversaw and provided her treatment. In part, the patient alleged that the care providers' failure to transfer her to a facility that could provide adequate and appropriate treatment constituted medical malpractice. The physicians admitted to being aware of the treatments and were familiar with research indicating the high success rate in preventing permanent injury due to asthma-induced hypoxia. The defendant physicians and hospital nevertheless denied liability. A jury concluded that the physicians and hospital were liable and awarded the patient $110 million for her injuries and continued required medical care.

What this means to you: This medical malpractice action focused on whether the defendant physicians' decision not to transfer the patient, who could have received different treatment at a better-equipped facility, constituted a breach of the applicable standard of care. The physicians were aware of the patient's condition and attempted to provide treatment, so this was not an issue of failing to provide any treatment or delay in providing the appropriate treatment. Rather, the physicians in this case were incapable of providing treatment such as ECMO or HFOV due to the limitations of their facility. Those treatments were readily available at other nearby facilities — a fact the defendant physicians knew.

At trial, the physicians and hospital presented an expert witness who testified that use of ECMO and HFOV to treat a patient in a similar condition is not the standard of care. In fact, the expert opined that such treatments would not be standard but were instead novel; the expert further claimed that salvage therapy and inhalation anesthesia — which were administered by the defendant care providers — was the appropriate course of treatment in the given situation.

The patient presented her own expert witness who offered an opinion in direct contradiction to the defendants' expert. According to the plaintiff's expert, the defendants' expert attempted to confuse the words "novel" and "salvage." As pointed out by the plaintiff's expert, the inhalation anesthesia administered by the physicians also is considered "salvage therapy" to the same extent ECMO would be considered part of such category. In this sense, the meaning of "salvage" must be interpreted as a therapy beyond that which is conventional — a therapy used to save critical, dying patients in a final attempt. The plaintiff's expert noted that this concept should not be confused with "novel" therapies, which include all untested and untried therapies.

Furthermore, the defendant's expert's submissions included a number of papers and scholarly articles indicating that ECMO had been used to treat severe cases of asthma since the 1990s. Additional research demonstrated how hospitals within the same geographic region had been consistently using this sort of treatment for years and had encountered a very high rate of success in saving patients suffering from severe asthma.

The two dueling experts in this case reveal another important lesson: Experts in medical malpractice are critical, and an expert can make or break a case. Here, the court found that the defendant's expert's opinion was inaccurate to the extent that ECMO and HFOV are not considered novel and have been in use since the 1970s. Such a determination necessarily undermines the expert's opinion generally, damaging the expert's credibility with the jury.

During their depositions, three of the physicians involved in the patient's care admitted that they knew of the existence and availability of ECMO treatment in a nearby facility, just miles away from the hospital where the patient received treatment. The physicians further admitted that had the therapy been available at the hospital, the plaintiff's brain damage could have been avoided. These facts demonstrated in part that the physicians' and hospital's care fell below the applicable standard. The jury agreed with the patient particularly because while the defendant physicians stated they had run out of options for the patient's treatment, they also stated that they knew about the existence and availability of ECMO; therefore, they should have considered transfer and made an attempt to prevent further damages.

In addition, the patient's expert explained that while HFOV treatment involved a higher level of risk, it was also not any more experimental than the inhalation anesthesia that was performed, and more hospitals are able to provide this type of treatment compared to ECMO. Thus, by the physicians' own admissions, because they had exhausted the possibilities available at the hospital in question, HFOV should have been attempted as it could have potentially prevented the patient from suffering permanent damage.

Hospitals are required by state and federal laws to not admit or transfer out patients who need a higher level of care than can be provided by the facility the patient is in. While this sounds simple enough, the process of transferring patients from one acute care setting to another is more complex: there must be bed availability, a physician must agree to accept and take over the care of the patient, insurance issues and payment sources must be acceptable, and so on. It is usually nursing staff supervisors or case managers who work on these arrangements. When there are patients who are not responding to standard treatments, efforts by care providers must be made expeditiously to consult with experts and get opinions on alternative treatment options that are available and accessible. It is much more prudent for a physician to get an expert's opinion while the patient is still under his or her care than to hear such opinion at trial — and the failure to timely seek out and implement such options may constitute medical malpractice. ■

REFERENCE

Decided on April 12, 2019, in the Supreme Court of the State of New York, Case Number 310294/11.