HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE SINCE 1979

INSIDE

RELIAS MEDIA

MAY 2019 Vol. 41, No. 5; p. 49-60

Subpoenas Require Response Plan, Staff Education on Proper Steps

Hospitals and health systems receive many subpoenas demanding information or the appearance of individuals in a legal matter, and it is easy to lose sight of how important it is to respond appropriately. Improperly responding to a subpoena can result in legal difficulties and damage the outcome of the related litigation.

The key to properly managing subpoenas is to create a formal policy that outlines how staff respond to this legal demand, says **Robert H. Iseman**, JD, partner with the Rivkin Radler law firm in Albany, NY. There must be a procedure in place for accepting any kind of legal process, including a summons that initiates a lawsuit, a subpoena from a party in litigation or perhaps from a public agency, he says.

> THE KEY TO PROPERLY MANAGING SUBPOENAS IS TO CREATE A FORMAL POLICY THAT OUTLINES HOW STAFF RESPOND TO THIS LEGAL DEMAND.

"Any kind of compulsory legal process ought to be presented to a particular office within a healthcare organization, such as the legal counsel's office, to accept process. The first benefit is making sure that it does not get lost, that you don't find yourself in default of a lawsuit or failing to produce the documents or person required by the subpoena simply because you never properly received it and had a chance to respond," Iseman says. "Many organizations don't have that."

These types of requests include civil and criminal subpoenas, administrative/regulatory subpoenas, and Civil Investigative Demands under the False Claims Act, explains **Matthew S. Arend**, JD, partner with the Dinsmore law firm in Cincinnati.

Financial Disclosure: Author **Greg Freeman**, Editor **Jill Drachenberg**, Editor **Jesse Saffron**, Editorial Group Manager **Terrey L. Hatcher**, 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: Terrey L. Hatcher
ACCREDITATIONS MANAGER: Amy M. Johnson, MSN, RN, CPN

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

Different types of requests — and different senders — carry with them different compliance obligations and privacy considerations, he says.

For example, regulatory requirements under HIPAA differ significantly if the request is made via a subpoena issued in a civil case versus one issued by a grand jury in a criminal proceeding or an administrative request by the Centers for Medicare & Medicaid Services (CMS) or Department of Justice (DOJ), Arend says. There may also be state law considerations, such as physician-patient privilege or the peer review privilege (and any exceptions to privilege), depending on what information has been requested.

Some subpoenas require the production of both a live witness and documents, Iseman notes. A healthcare organization's policy should be tailored to account for the various types of subpoenas that might be received and how they require different types of compliance, he says.

Substance Abuse Laws Are Strict

Of particular concern are subpoenas that may involve substance abuse records, which are protected in ways other medical records are not.

"There is a longstanding series of federal statutes and regulations that protect substance abuse records, prohibiting a hospital that may have a drug rehabilitation program from producing any of those records unless there is a consent form in the file that has been signed by the patient and which meets very specific and rigorous requirements," Iseman says. "Many organizations don't have a consent form on file that meets the requirements of the law. One of the reasons is that the consent form must specifically designate the person to whom the information can be released, rather than a blanket consent form."

Without such a consent form, the hospital is required to inform the party issuing the subpoena that federal law precludes responding to the subpoena, Iseman explains. In such a situation, the law prohibits even acknowledging that the person is a patient at the facility, he says.

Iseman says the appropriate response would be something like this: "Without conceding that Joe Smith is now or ever has been a patient at the facility, the information sought by the subpoena refers to protected substance abuse

EXECUTIVE SUMMARY

Hospitals and health systems should have a formal policy on responding to subpoenas. Staff must be educated on how to properly respond when presented with a legal demand for material or a court appearance.

- There is a difference between a subpoena issued by a court and one issued by an attorney.
- Policies and procedures should ensure that you comply only with what the subpoena requires.
- Specific laws regarding some records and state laws may affect subpoena compliance.

information, and we do not have a consent which permits us to disclose any records." The issuing authority would then have to seek a court order for the records, which would be granted only in extreme cases such as when it is required to prevent child abuse or serious crimes, he explains.

"The court order is not going to be issued for a garden-variety divorce proceeding, for instance, in which a spouse is alleging substance abuse by the other party," he says. "The grounds for the court to issue the order are so narrow that it is a very high bar."

Subpoena compliance also can be governed by HIPAA requirements, Iseman says. While they are not as restrictive as the substance abuse rules, they can preclude turning over as much information as requested in a subpoena. There also can be additional restrictions from laws related to HIV and mental healthcare, he notes. Many of these vary from state to state.

State Laws Can Allow Private Action

One factor working in favor of healthcare organizations is that the federal rule on substance abuse confidentiality does not provide a private right of action, Iseman explains. The rules are enforced by the DOJ, so there is the risk of federal fines, but private litigants cannot sue for compensation. Likewise, people cannot sue civilly under HIPAA.

However, there can be a private right of action under parallel state laws, Iseman explains. That can pose significant liability under a common law claim, he says.

"There must be adequate training of any staff who might be involved in receiving or responding to a subpoena, and one of the first steps is to determine if what the subpoena is demanding can be released," Iseman says. "You can't assume that the attorney issuing the subpoena knows the law and so it must be OK to release the records. We have cases in which the healthcare organization shows up in court and says they can't release the records because of this law, and the judge doesn't even know about the law."

Iseman says he suspects most healthcare risk managers and legal counsel have heard of the additional restrictions that govern some subpoena compliance, but merely being familiar with those laws may not be enough.

"Whether they are organized enough to have a process and procedure to address them is another matter entirely," Iseman says. "Whether that process works is also another matter that is uncertain."

Designate Individuals for Subpoenas

Many healthcare organizations designate one or two people in the legal counsel's office to receive and respond to subpoenas, Iseman says. That person should be familiar with the basic requirements of the law, as well as the hospital's policies and procedures, and know when to seek additional legal counsel before responding.

Depending on the size of the organization and the type of request, Arend says the responsible party also can be in the records department, risk management, or legal staff. All hospital staff should be trained to immediately direct any requests for records to the designated person(s) for handling.

"Those handling the responses should be further trained on how to differentiate run-of-the-mill requests from those requesting more sensitive information or those which may require special handling, such as psychiatric or psychotherapy records or substance abuse treatment information covered under 42 CFR Part 2," Arend says. "Responses should be logged, not only to track receipt and response dates but also to document when and to whom records were provided as required by certain regulations, including HIPAA, which requires organizations to keep an accounting of all disclosures."

Rely on Counsel When Necessary

When in doubt, contact legal counsel, Arend says. Whether the organization relies on inside counsel or an outside attorney, having an expert with significant knowledge and experience in this area can be a lifesaver, he says.

"Penalties for unauthorized disclosures can be severe and, unfortunately, good intentions or misunderstanding of the law won't necessarily save you from enforcement. I serve as outside privacy counsel for a number of healthcare clients, and I often work hand-in-hand with them in solving the more thorny dilemmas that can arise," Arend says.

"Often, disclosure involving law enforcement can be the most tricky for healthcare organizations to address. They want to cooperate and foster a good relationship with law enforcement, yet they are also bound by various privacy regulations that law enforcement may not be well-versed in or particularly care about."

In those situations, having counsel

to serve as a buffer and a sort of translator regarding the law can help to resolve disputes and prevent misunderstandings, he says.

"For example, I represent a local behavioral health practice that regularly receives subpoenas for information and testimony from the local prosecutor's office for various child welfare proceedings. Obviously, this is an area rife with risk: mental health, substance abuse, information relating to minors, etc.," he says. "However, in order to avoid having to take an unnecessarily adversarial stance, I was able to reach out to the prosecutor's office and get them to agree to implement a procedure where they would reach out to my office to discuss the matter prior to issuing a subpoena in order to discuss the requests and to make sure they had all of the proper documentation and authorizations we would need to comply with their requests."

Utah Case Still Worries Some

The greatest risk related to subpoenas comes when law enforcement officers demand immediate response, Arend says.

"The various overlapping regulations, exceptions, and public policy goals can sometimes make for a murky environment where the requirements for proper compliance aren't always immediately clear. In those situations, I recommend engaging outside counsel to help work through the issue," he says.

Recently, a hospital client reached out to Arend with concerns that police were bringing in DUI suspects with signed search warrants and demanding that hospital personnel draw blood samples and provide them with the results, Arend notes. This was reminiscent of a highly publicized incident in Utah in 2017 in which a nurse was arrested for following hospital policy and refusing police orders to draw blood samples.

That case illustrated what some healthcare professionals said was a common dilemma. The images of the Utah nurse being forcibly arrested as she begged for help still linger with many in the industry. *(For more information on the Utah incident, see the story on page 53.)*

The hospital Arend worked with was uncomfortable participating in the process and especially with frontline emergency nursing staff being asked to parse whether their participation was appropriate.

"I was able to reach out to the city's law director to discuss the issue and to establish a set of procedures that would be used in order to remove the decision from healthcare personnel and elevate it to risk management to ensure uniformity in the hospital's response to these sorts of requests," Arend says. "In both of these cases, being proactive and spending time and resources on the front end of the issue likely avoided more significant legal and financial headaches down the road."

Arend says policies and procedures should address each of the types of requests the hospital is likely to see, include guidance on how such requests should be routed for a response, include a list of requirements to determine whether the request is valid, and address any exceptions to regulatory restrictions and any sensitive or highly protected categories of information that may require special handling under state or federal law. The policy should also outline procedures for production, including time frames (allowing time for objections, if necessary), any review protocols, format of production, and how to log the disclosure.

"Another difficult area can be the overly aggressive attorney who thinks they understand the law and is convinced that your objections and concerns are simply obstinacy on your part," Arend says. "Having a clear policy on which to rely, proper training, and a clear understanding of how the regulations work together and where the friction points exist between them can help risk managers and/or their legal counsel educate the requester and hopefully negotiate an acceptable resolution that also allows the hospital to remain compliant with its obligations to patient privacy."

Be Conservative With Subpoenas

Be conservative when responding to a subpoena for medical information, says **Lucie F. Huger**, JD, an officer, attorney, and member of the healthcare practice group at Greensfelder, Hemker & Gale in St. Louis.

"My first piece of advice is to review the subpoena to see whether the healthcare organization is named as a party — a plaintiff or a defendant — in the subpoena received by the risk manager," Huger says. "If the healthcare organization is named as a party, the risk manager will want to notify legal counsel for the healthcare organization that the subpoena has been received and then take direction from the organization's legal counsel before responding."

Before responding to a subpoena, it also is necessary to determine whether the subpoena is enforceable in the jurisdiction where the healthcare entity is located, Huger says. Generally, if the subpoena is

issued from a court that is out of state, it may not be enforceable.

"If the risk manager has concerns as to whether the subpoena is enforceable, then my advice is for the risk manager to share the subpoena and the concerns with the organization's legal counsel and then take advice from counsel as to an appropriate response," she says.

Assuming the subpoena is valid, the healthcare organization's response will depend on how the subpoena has been issued and who is seeking the information, she says. Generally, if the subpoena is signed by a judge, the healthcare organization will need to comply with the terms of the subpoena because it would likely hold the weight of a court order.

Failure to comply with a validly issued court order could result in fines or penalties against the healthcare organization.

"If the subpoena is not signed by a judge, which is more common, then the risk manager will need to determine whether it is a subpoena issued by a lawyer who is representing the former patient or whether the subpoena is coming from someone who is representing a person who is not the former patient," Huger says. "If the subpoena is issued by a lawyer representing the former patient seeking the medical records of the former patient, then a HIPAA-compliant authorization generally accompanies the subpoena."

In this scenario, it will be important to review the authorization to ensure that the former patient authorized the release of the subpoenaed information. If there is any question about the authenticity of the authorization or the scope of what is being requested, the risk manager should contact the former patient to ensure he or she authorized the information to be shared with his or her attorney through the subpoena.

"If the former patient confirms this, depending upon the level of concern, the healthcare organization may prefer to have the former patient sign the authorization form used by the healthcare organization and then produce the information to the attorney representing the former client," she says. "If there is not an authorization accompanying the subpoena from the attorney representing the former patient, my advice is to follow the same procedure — that is, have the former patient sign the appropriate authorization and then produce the records to the attorney representing the former patient."

On the other hand, if the subpoena is issued by a person who is not representing the former patient, Huger advises determining whether the former patient, through his or her attorney, has authorized the release of this information. Again, if the former patient agrees to the release of this information, then the risk manager will want to receive a signed authorization from the patient.

If there is any question as to whether the former patient has authorized the release of his or her information, the hospital should seek a court order, she adds.

Huger says she has seen hospitals

Notorious Nurse Arrest Still Causes Subpoena Worries

It was far from the first time a nurse was put in a difficult situation with a police officer demanding she do something, but the 2017 case of nurse Alex Wubbels, RN, was a sensational illustration of how much can go wrong.

The Wubbels case drew attention to hospital policies and procedures regarding subpoenas and other demands from law enforcement, particularly how frontline clinicians can be left on their own to refuse sometimes aggressive police officers. The arrest of Wubbels was even facilitated by her own hospital's security guards.

Wubbels was a charge nurse at the University of Utah Hospital in Salt Lake City. Police detective Jeff Payne demanded hospital staff draw blood from the patient, or he wanted to do it himself because he worked off duty as a paramedic and the police department authorized him to draw blood for investigations.

Wubbels refused, explaining that she could not allow the blood draw without a warrant or the patient's permission. Payne arrested Wubbels, dragging her out of the hospital as she cried for help. Hospital security guards stood by without helping, and one opened a door for Payne as he took Wubbels out.

The police department fired Payne and demoted his supervisor to officer. The city settled with Wubbels for $500,000. Payne told media outlets in November 2018 that he was not sorry for his actions.

For more on the Utah case, see "Nurse Arrest Puts Focus on Hospital Security, Policies" and related stories in *Healthcare Risk Management*, November 2017, available online at: https://bit.ly/2IccmU6. ■

respond well to complex subpoena situations, and others have performed poorly.

"Generally, those who appropriately respond take the steps necessary to ensure that only responsive information is provided to people who have demonstrated a legal right to having the information and have taken the correct steps to ensure this," she says. "On the other hand, I have seen poor responses because a risk manager did not understand the difference between a subpoena and a court order. Unfortunately, once information is wrongfully disclosed, this can be very difficult for the person whose information was disclosed." ■

SOURCES

- **Matthew S. Arend**, JD, Partner, Dinsmore, Cincinnati. Phone: (513) 977-8388. Email: matthew.arend@dinsmore.com.
- **Lucie F. Huger**, JD, Officer, Greensfelder, Hemker & Gale, St. Louis. Phone: (314) 345-4725. Email: lfh@greensfelder.com.
- **Robert H. Iseman**, JD, Partner, Rivkin Radler, Albany, NY. Phone: (518) 641-7055. Email: robert.iseman@rivkin.com.

Use Claims Analysis to Find Actionable Data, Not Just Global Data

Eighty percent of physicians will face a medical malpractice lawsuit at some point, with those in high-risk specialties like obstetrics facing even worse prospects. Risk managers welcome any strategy that helps identify the physicians and situations most likely to result in liability.

Closed claims are an invaluable resource for identifying risks, highlighting the most common factors associated with adverse outcomes and liability. Like other organizations, TeamHealth, based in Knoxville, TN, with more than 20,000 clinicians nationwide, has used closed claims data analysis to help identify those risks and potential risk reduction opportunities.

But there is a limit to the information that can be gleaned from closed claims, says **Kevin Klauer**, DO, EJD, FACEP, chief medical officer for hospital-based services and chief risk officer with TeamHealth.

"Those databases are not specifically designed to identify risk trends," Klauer says. "You can get high-level numbers like the claims in a certain area geographically, or with a certain diagnosis. But when it comes down to moving toward predictive modeling and getting actionable information for physicians, you need more."

For instance, Klauer says it is not enough to remind physicians that stroke, sepsis, and heart attacks are often misdiagnosed or mismanaged simply because the closed claims data indicate those are frequent topics in civil litigation. Physicians are already trying to manage those issues properly, so simply telling them that they often result in lawsuits is not much help, he says.

"You have to give them actionable data, information that is useful clinically, rather than just saying 'Here's a problem, and here's some reminders about best practices,'" Klauer says.

"You're also implying that the clinician did something wrong, and we know in claims management that is not always the case," he adds. "These are multifactorial claims, and frequently, there is nothing wrong with the care provided. But you still have a very unhappy patient who is unsatisfied with the outcome."

Claims Database Improved

To collect more actionable data, TeamHealth added additional data fields retrospectively to the claims analysis. The goal was to derive data that were more useful for predictive modeling and risk management, Klauer says.

For example, the data analysis indicated that sepsis was the chief readmission complaint of ED

EXECUTIVE SUMMARY

Closed claims analyses can have limitations when recommending improved practices for clinicians. Strive for actionable information rather than global data.

- It may be necessary to improve data points in closed claims before analysis.
- Seek specific results that may be counterintuitive.
- Avoid telling clinicians to just be more vigilant.

patients. TeamHealth had already provided that information to its clinicians, along with reminders about best practices for sepsis prevention, and Klauer says that is necessary. But they wanted to go further.

"You can't stop there. We also include in our database now, and we retro-populated it, the chief complaint when someone came in to the emergency department and was ultimately diagnosed with sepsis," Klauer explains. "And what was the physician diagnosis given when they left that ultimately resulted in a diagnosis and a lawsuit for sepsis? That's actionable information, and it may return some information that is counterintuitive."

With sepsis, for instance, Klauer notes that it is reasonable to assume sepsis will be diagnosed in patients with undifferentiated fever. But interestingly, that was only the second most common complaint in patients who were discharged and returned later with sepsis. The number one complaint was abdominal pain, which can be especially difficult to pin down with a diagnosis.

UTIs Discovered as Sepsis Link

Once abdominal pain patients return with sepsis, the analysis indicated that the most common diagnosis was urinary tract infection.

"That is incredibly actionable information. You can tell your physicians that if they have examined a patient with abdominal pain and sent them home with a diagnosis of urinary tract infection, there is a subset of those patients who will return with sepsis," Klauer says.

"Frequently, the urinalysis they did during the examination for abdominal pain will have had some nonspecific findings like a few white blood cells or maybe some nitrates. Those are not always diagnostic, but you can anchor on them and that might raise your suspicion of urinary tract infection."

In the vast majority of patients with a urinary tract infection diagnosis after returning with sepsis, there were no urinary symptoms of that infection when they originally sought care for abdominal pain, Klauer says.

"So instead of telling clinicians that 'sepsis is a concern and it's a better diagnosis, please keep that in mind and do a better job,' it is more useful to tell them that when you may miss sepsis is in this situation: You have a patient with undifferentiated abdominal pain who got a thorough evaluation, you thought they might have a urinary tract infection, and you sent them home," Klauer says. "Give them actionable information rather than just global information. Mindfulness is not a risk management strategy." ■

SOURCE

- **Kevin Klauer**, DO, EJD, FACEP, Chief Medical Officer for Hospital-based Services, Chief Risk Officer, TeamHealth, Knoxville, TN. Phone: (800) 342-2898.

CRNAs Manage Risk Through Improved Consent, Documentation

Certified registered nurse anesthetists (CRNAs) face liability risks unique to their profession, and risk managers can assist them by reminding them of the potential pitfalls in their work and the best ways to minimize their exposure.

CRNAs are among the most vulnerable in the nursing profession because their high skill level affords them greater autonomy, notes **Georgia Reiner**, risk specialist for the Nurses Service Organization (NSO) in the Healthcare Division of Aon Affinity Insurance Services in Philadelphia. With that autonomy comes greater responsibility for adverse outcomes and potential liability.

The NSO recently highlighted a case study of a CRNA who performed a peribulbar eye block on an ambulatory surgery patient prior to his cataract surgery. After an adverse outcome, the CRNA was the only clinician sued. When the patient refused to settle for less than $500,000, the matter went to trial. Even though the trial ended with a defense verdict, the estimated legal fees after three years were $270,000. *(For more on that case and the risk management implications, see the case study online at: https://bit.ly/2GfvdeQ.)*

"Risk management's role is to be the informer, helping to improve patient safety and minimize exposure by providing information on the patterns and trends and losses we see," Reiner says. "We hope that risk managers can use the information

from NSO to help evaluate the risk exposures that they have identified in their organizations and implement changes that will lead to better outcomes for their patients and reduce liability for the organization, as well."

Reiner suggests educating CRNAs on the following strategies for avoiding liability:

• Stay on top of staff experience, training, and skills, monitoring for continuing education.

Policies and procedures should be in place to regularly assess the education and training needs of staff, and evaluate each professional's credentials and competencies, she says.

"It behooves the CRNAs themselves to maintain their education and skills, but it also behooves the organization to support that process by having policies and procedures in place that assess the education and training of their staff to evaluate where any gaps may exist," Reiner says. "It is important for organizations to support that process because when you have a well-educated, skilled workforce, everyone benefits."

• Document informed consent for every procedure involving anesthesia.

CRNAs should verify that informed consent was obtained and documented in the patient's health record. Risk managers should confirm that verification of this informed consent process is part of any checklist or time-out procedure completed before an anesthetic intervention.

POLICIES AND PROCEDURES SHOULD BE IN PLACE TO REGULARLY ASSESS THE EDUCATION AND TRAINING NEEDS OF STAFF, AND EVALUATE EACH PROFESSIONAL'S CREDENTIALS AND COMPETENCIES.

"It's important to look at policies and procedures and make sure they support any work the healthcare provider is doing with patients, so obtaining feedback from providers about potential gaps is important," she says.

"If you don't seek that feedback, it is possible that you have conflicts or shortcomings with your policies and procedures that CRNAs know about — and you could correct if you ask them."

• Note any pertinent anesthesia-related information on the patient's record, including allergies.

Risk managers can work with clinical directors and health information management to ensure that pertinent information can be effectively recorded in the patient's health record and appropriate alerts are in place to notify practitioners of any urgent concerns, such as allergies or potentially adverse drug interactions.

"We know that some of the top allegations made against CRNAs in malpractice lawsuits involve improper treatment or intervention, or inadequacies in the anesthesia plan," Reiner says. "We have identified that documentation can be lacking, and when it is, that makes defense of the CRNA much more difficult."

• Continually monitor the patient's status and response to treatment, and report changes in a timely manner.

"Sometimes we see a failure to provide and document to the practitioner a change in the patient's status," Reiner says. "That breakdown in communications can lead to adverse outcomes for the patient."

• Document practitioner notification of status changes.

CRNAs must report changes in the patient's condition, any new symptoms, or any patient concerns to the practitioner in charge of the patient's care, Reiner says. CRNAs also should document the practitioner's response and any orders in the patient's health record.

"Risk managers and organizational leadership should work together to identify barriers to effective team functionality and design systems that help foster

EXECUTIVE SUMMARY

Educate certified registered nurse anesthetists (CRNAs) about their unique malpractice risks. Their elevated education provides autonomy that can make them likely targets of litigation.

- Maintaining competency and skills is a top priority.
- Lax documentation is at the root of many CRNA lawsuits.
- Communication about the patient's condition can be another weak point with CRNAs.

collaborative, patient-centered healthcare teams and improve communication among healthcare professionals," Reiner says.

"To that end, risk management programs should include an educational component to help engage staff in improving the quality and safety of care at their organization."

Patient safety initiatives and educational programs such as Team Strategies and Tools to Enhance Performance and Patient Safety (TeamSTEPPS) and Quality and Safety Education for Nurses (QSEN) can improve communication and teamwork among healthcare professionals, and between providers and patients, Reiner suggests.

• Report any patient incident, injury, or adverse outcome.

Rather than blaming individuals when errors or near-misses occur, risk managers should promote shared accountability and engage healthcare providers in the process of understanding the causes of errors. Risk managers must encourage CRNAs and other healthcare providers to report any patient injury or adverse incidents, as it is only through the incident reporting and root cause analysis process that patient care and treatment practices can improve, Reiner says.

"Risk managers should also encourage CRNAs to alert their professional liability carrier to any potential claims, as timely reporting ensures that an incident, if it develops into a covered claim and is not excluded for other reasons, will be covered," Reiner says. "Rather than focusing on blaming individuals for any particular error or liability, risk managers should promote shared accountability to understand the root causes of errors. To foster that environment, risk managers should encourage CRNAs to report any near misses or adverse outcomes without fear of retribution." ■

SOURCE

- **Georgia Reiner**, Risk Specialist, Nurses Service Organization, Healthcare Division, Aon Affinity Insurance Services, Philadelphia. Email: georgia.reiner@aon.com.

Cryptojacking Among Latest Cyberthreats for Healthcare

The world of cybersecurity continues to evolve, with hackers now using approaches unfamiliar to risk managers. Staying ahead of the hackers is a challenge, particularly with nation-states getting more involved with the attacks on hospitals and health systems.

Hackers are rapidly developing new ways to intrude on healthcare IT systems, says **Ophir Zilbiger**, partner and head of SECOZ Cybersecurity Center with BDO Israel in Tel Aviv. In some cases, their motivation has changed from obtaining patient data to using the healthcare organization's computing power for illegal purposes.

BDO's recent report, *Brace for the Breach*, summarizes new developments in cybersecurity. *(The report is available online at: https://bit.ly/2D4VqLg.)* Key findings from the report include the following:

• More decentralized cyberattacks. Rather than targeting the hospital or health system directly, these attacks compromise a healthcare vendor's technology or network connections. Once they have access, the hackers can penetrate the network of the vendor's customers — the hospitals and health systems. This is now the favored approach of hackers, according to the report.

Medical device recalls as a result of corrupted software have increased 126% since the fourth quarter of 2017, the report says. The legacy systems in many healthcare IT infrastructures are geographically dispersed, which multiplies opportunities and venues for cyberattacks.

• Nation-states are increasingly involved with cyberattacks on hospitals. Instead of targeting prominent clinics that may treat politicians and other notable patients and have formidable security, they

EXECUTIVE SUMMARY

New threats are emerging in cybersecurity. One risk for healthcare organizations involves using the victim's computing power.

- Cyberattacks are targeting healthcare organizations' vendor networks.
- Nation-states are more involved with sponsoring cyberattacks.
- Cryptojacking can be used to mine bitcoins.

target smaller rural hospitals located close to decentralized facilities such as military bases. The goal is steal the records of military leaders, clinical trial research, and sensitive information such as that related to biological weapons. Only 7% of 475 hospital CEOs surveyed knew nation-states were among the top three cyberadversaries.

• **Cryptojacking is a growing threat, but it is not well-known in the healthcare community.** In cryptojacking, malware is introduced to a healthcare organization's computer system not to steal data but to take advantage of the computing power and network resources. The most common purpose is for the mining of bitcoins, which requires significant computing power.

• **The top seven categories of cyberattacks in healthcare are denial of service attacks, business email compromise, supply chain attacks, internal threats, cryptojacking, ransomware, and computer intrusions.**

Cryptojacking is among the most worrisome threats, Zilbiger says. The increasing use of blockchain technology makes the computing power of healthcare organizations appealing to hackers, he says.

"Hackers today are mostly about making money. Not so many years ago, we were talking about hackers making their reputations with these attacks, becoming famous in their communities for political reasons," Zilbiger says.

"Now they are about making money, and many are employed by criminal organizations. They can simply steal money from cryptocurrency owners, but they use cryptojacking to create money. In the cryptocurrency world you can mine, or create, additional money, but it takes tremendous resources in terms of the hardware and electricity."

The amount of energy required to mine a bitcoin can be more than the bitcoin's value, Zilbiger says. But that is not a problem if the hacker is using a hospital's IT system to mine bitcoins. The threat to the healthcare organization comes when that vast amount of computing power is drawn from the IT system and threatens the normal operations involved with patient care and administration, he explains.

"We're seeing more and more of this," Zilbiger says. "The way the cryptojackers get into the system is the same as from other cyberthreats, so the defenses are largely the same. You do not have to be a massive organization to be threatened by cryptojacking because they also have the ability create a network in which they draw computing capacity from many users, even individuals at home, and combine it to create the computing power they need to be profitable with mining cryptocurrency." ■

SOURCE

- Ophir Zilbiger, Partner, Head of SECOZ Cybersecurity Center, BDO Israel, Tel Aviv. Phone: (972) 52-6755544. Email: ophirz@bdo.co.il.

Hospital Apologizes to Patients Videotaped in Gynecological Procedures

A California hospital has apologized to more than 80 women who filed a class-action suit claiming the facility recorded them during gynecological procedures without their knowledge or consent.

The hospital had been trying to catch someone who was stealing drugs from anesthesia carts on the surgical unit, and the motion-activated cameras inadvertently recorded women during clinical care in three operating rooms.

The surveillance continued for a year and captured more than 14,000 video clips before administrators realized the cameras were recording patients and removed them.

"Although the cameras were intended to record only individuals in front of the anesthesia carts, others, including patients and medical personnel in the operating rooms, were at times visible to the cameras and recorded without sound," according to the statement issued recently by the hospital. *(The hospital's statement can be found at: https://bit.ly/2v9Ia3v.)*

More than 80 women filed a class-action lawsuit in 2016, including one who said her emergency cesarean section was recorded by the cameras. The video recordings were kept in a "secured safe" until they were turned over as part of a state investigation and the civil litigation, the hospital said.

The cameras did catch the person stealing drugs, and that person is no longer associated with the hospital, the statement said.

For more on the case, see "Drug Diversion Sting Goes Wrong And Privacy Is Questioned" in the July 2016 issue of *Healthcare Risk Management*, available at: https://bit.ly/2uSQS6j.

HHS Warns of Advanced Persistent Threats, Zero-Day Exploits

The Department of Health and Human Services Office for Civil Rights (OCR) is warning about the threat to healthcare organizations from advanced persistent threats (APTs) and zero-day exploits (ZDEs).

OCR recently called attention to increased risk from these two cyberthreats. It describes an APT as "a long-term cybersecurity attack that continuously attempts to find and exploit vulnerabilities in a target's information systems to steal information or disrupt the target's operations."

APTs Not Advanced, but Persistent

The APT may not be especially advanced from a technological perspective, but the relentless attack can eventually find a weakness to exploit, and changing tactics can make the overall attack difficult to detect.

"APTs are a serious threat to any information technology (IT) system but especially those that are part of the healthcare field," according to the report. "APTs have already been implicated in several cyberattacks on the healthcare sector in the U.S. and around the world."

ZDEs Find Vulnerability

OCR also cautions that ZDEs are "one of the most dangerous tools in a hacker's arsenal." This is a type of hacking that takes advantage of a previously unknown hardware, firmware, or software vulnerability before corrections can be made or defenses mounted.

The weaknesses sometimes are discovered by hackers performing their own research, or they may act quickly once an opening is discovered, trying to take advantage before a patch or antivirus solution can be provided to users.

"These exploits are especially dangerous because their novel nature makes them more difficult to detect and contain than standard hacking attacks," OCR says.

"The possibility of such an attack emphasizes the importance of an organization's overall security management process which includes monitoring of antivirus or cybersecurity software for detection of suspicious files or activity."

The full OCR report is available online at: https://bit.ly/2X3zh7P. ■

800 Hospitals Dinged by Medicare for Hospital-Acquired Conditions; Payments Held

Medicare is making good on its promise to withhold payments under the Hospital-Acquired Condition Reduction Program. The latest figures show 800 hospitals are not getting their expected reimbursement because of patient safety failures.

Since the program began, Medicare has penalized 1,756 hospitals at least once. In 2019, 110 hospitals are being denied payments for the fifth straight year.

Hospitals are compared against one another for rates of six HACs: central line-associated bloodstream infection, catheter-associated urinary tract infection, surgical site infection from abdominal hysterectomy or colon surgery, methicillin-resistant *Staphylococcus aureus* (MRSA), and *Clostridioides difficile* infection. Medicare withholds some payment from the 25% with the worst rates each year.

Improvement from the previous year does not help if the hospital still remains in the worst quartile.

Each hospital in that category will have 1% of its potential Medicare payments deducted for patients discharged between October 2018 and September 2019. The latest data on the HACRP is available online at: https://bit.ly/1QhKT0Z. ■

COMING IN FUTURE MONTHS

- Avoiding violations of the Fair Labor Act
- ACA requirements for healthcare employees
- Common informed consent challenges
- Top malpractice risks in anesthesia

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 instantly.

CME/CE QUESTIONS

1. **According to Robert H. Iseman, JD, when would a court be likely to require the release of patient records related to substance abuse without the patient's consent?**

   a. Any time the request comes from a law enforcement agency.
   b. Any time the request is sufficiently related to ongoing litigation.
   c. Only in extreme cases such as when it is required to prevent child abuse or serious crimes.
   d. Only after the death of the patient.

2. **What does Kevin Klauer, DO, EJD, FACEP, say risk managers should seek in a closed claims analysis?**

   a. Actionable information for clinicians
   b. The most recent data
   c. Data that pertain only to a local geographic area
   d. Data derived only from cases in which the clinician clearly made an error

3. **According to Georgia Reiner, why do CRNAs face a higher risk of malpractice liability?**

   a. They often act beyond their scope of practice.
   b. They often are inadequately supervised.
   c. Their elevated level of education and autonomy makes them a target for plaintiffs.
   d. Their credentials were not adequately verified before allowing them to practice.

4. **What is the purpose of cryptojacking?**

   a. To steal patient data
   b. To harness the resources of the computer system to mine cryptocurrency
   c. To steal information related to military leaders
   d. To destabilize the computer system and demand ransom

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

Patient Settles With Hospital and Physicians for Alleged Malpractice Leading to Paralysis

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 58-year-old male presented to a hospital with abdominal pain, nausea, and vomiting. He was otherwise in good health and able to perform all daily activities without assistance. A CT scan revealed several aneurysms, but two radiologists failed to detect that one had already ruptured. The patient's condition rapidly deteriorated, and despite an emergency surgery, the patient suffered permanent paralysis.

The patient and his wife brought suit against the hospital and multiple physicians, alleging that their failure to diagnose and treat the ruptured aneurysm constituted medical malpractice. The defendants denied liability. Six days prior to the start of trial, the parties entered into a settlement agreement for a total of $20.6 million.

Background: In October 2013, a 58-year-old man was admitted to the ED with abdominal pain, nausea, and vomiting. A CT scan was performed on his abdomen, revealing several aneurysms. According to the patient, two radiologists who reviewed the scan failed to notice that one of the aneurysms was already bleeding. A vascular surgeon reviewed the scan the next morning and also failed to notice the bleeding aneurysm.

As the day progressed, the patient's condition worsened. He experienced weakness in both legs, a severe drop in blood pressure, even more severe abdominal pain, abdominal distension, and a decrease in hemoglobin and hematocrit. The following morning, the patient's condition had further worsened as he experienced increased weakness in his lower limbs. The attending day hospitalist, suspecting a spinal epidural abscess, ordered a routine MRI; however, it was not performed due to severely increased abdominal distension. The physician ordered an immediate X-ray, which showed a dilated large bowel. The patient was promptly transferred to a different hospital where another CT scan showed a rupture in the patient's right common iliac artery aneurysm.

THE PATIENT SUFFERED BILATERAL FASCIOTOMIES ON BOTH LEGS, AMPUTATION OF SEVERAL TOES, DEEP PRESSURE ULCERS, AND CHRONIC PAIN. HE ALSO WAS LEFT PERMANENTLY PARALYZED.

Emergency surgery was performed to fix the rupture; however, it was too late to prevent all injuries. The patient suffered bilateral fasciotomies on both legs, amputation of several toes, deep pressure ulcers, and chronic pain. He also was left permanently paralyzed. The patient requires full-time assistance and care, and is unable to work as a result of his injuries.

In 2015, the patient and his wife filed a medical malpractice action against the initial hospital and several of the individual physicians who were involved in his care. The patient alleged that the physicians did not provide him with the necessary standard of care and that their negligence caused him to be rushed into surgery, which resulted in the significant, permanent injuries.

The defendant hospital and physicians claimed that because the patient suffered from end-stage kidney disease,

his life expectancy was already significantly diminished. They further asserted that the patient's injuries were well-known complications of the surgery he required. Finally, the defendants argued that the surgery was necessary regardless of when the bleeding aneurysms were diagnosed and the patient's injuries were no more severe as a result of the delayed diagnosis.

Six days before the trial, the parties entered into a complete settlement agreement, resolving all of the patient's claims against the hospital and individual physicians. The hospital agreed to pay the patient $13.5 million, and the physicians collectively agreed to pay $7.1 million, for a total of $20.6 million.

What this means to you: This case serves as an example of both the importance of ensuring that information on a patient is clearly communicated among physicians and staff when multiple physicians are involved in the care of the patient, as well as the importance of timely diagnosis and prompt treatment. The sizeable settlement reached by the parties is confirmation of the significance of the patient's injuries and the significant possibility of liability on behalf of the hospital and physicians.

In this case, from the time the patient was admitted to the ED to the time surgery was performed, the patient was seen and treated by numerous physicians. This situation, which is especially common in an ED setting, can lead to difficulties in patient information being communicated correctly and increased times in diagnosis. In fact, among other things, the patient alleged that three different physicians revised his initial CT scan and that all three failed to notice that one of the aneurysms in his abdomen was already bleeding at the time. Also, the physician who treated the patient the next morning had not previously examined the patient and did not properly assess the speed at which the patient's condition was worsening. This is evidenced by the fact that the doctor, according to the plaintiff, ordered a routine MRI rather than a stat MRI, which would have been appropriate given the patient's newly developed symptoms.

Further, the scheduled routine MRI was never performed because within 12 hours, the patient's condition had become so severe that he had to be transported to another hospital to undergo emergency surgery. Had a single physician adequately monitored the patient's condition or had the information been communicated more accurately among the multiple physicians, the gravity of the patient's condition may have been noticed earlier, and a stat MRI would have been performed.

Physicians rely on quantitative and qualitative data they receive from nurses who are with patients for eight to 12 hours at a time. While one or more physicians on any case spend minutes with patients, nurses have the ability to observe trends in a patient's condition over time. Significant changes in a patient's condition must be reported to physicians rapidly and consistently until interventions are performed to address urgent conditions. A drop in blood pressure accompanied by a drop in hemoglobin and hematocrit levels are textbook signs of bleeding and possible hemorrhaging. Abdominal distention gives care providers a clue as to the area of bleeding.

This patient's body was providing signals about what was happening, but none of the physicians or staff involved recognized and reported them. The nurse assigned to this patient had a responsibility to notify the physicians about these critical changes and to follow up, using the chain of command if necessary, until appropriate actions were taken — in this case, emergency vascular surgery. All of these factors certainly affected the patient's course of treatment, and under different circumstances, it is plausible that the rupture of the aneurysm in his right common iliac artery could have been prevented and injuries reduced.

Regardless of the events, it is important to keep in mind that the initial delay in reaching a proper diagnosis and developing an effective course of treatment was most likely due to the fact that all three physicians who analyzed the plaintiff's CT scan failed to notice bleeding was already present. While this may not have entirely prevented the complications that subsequently developed, it may have resulted in the hospital staff checking in on the patient more frequently or noticing changes in his health more promptly. Since this matter settled prior to a finding of liability by a jury, it is difficult to evaluate the arguments and defenses raised by the parties.

Given the patient's significant and permanent injuries, and the delays by the physicians, a jury may well have determined that the physicians failed to provide care consistent with the appropriate standard. However, the physicians and hospital had plausible defenses concerning causation: If the patient would have suffered the same injuries regardless of the delay, then the injuries were merely an unfortunate unavoidable consequence of the patient's condition, and there was no negligence.

Medical malpractice trials are inherently risky and difficult to predict, as the patient and care providers must have appreciated.

These inherent risks and difficulties — as well as the costs of trial — encourage parties to settle matters before trial to greater control the potential for recovery, from a patient's perspective, and to control the amount of a verdict, from a care provider's perspective. Settlement discussions take place at all stages of litigation, even after trial has started. In this case, the parties had prepared for trial and thoroughly evaluated their claims and defenses, as well as the opposing side's claims and defenses, and determined that settlement was in all the parties' interests. This is a regular occurrence in litigation, and physicians and hospitals should consult with counsel to evaluate and determine whether settlement is appropriate for a specific case. ■

REFERENCE

Announced on Feb. 19, 2019; action in the Circuit Court of Cook County, Illinois, Case Number 2015-L-010132.

Appellate Court Confirms Surgeon Not Negligent in Performing Laparoscopic Cholecystectomy

News: A patient suffered from intermittent abdominal pain and was diagnosed with an abnormally functioning gallbladder. A physician performed a laparoscopic cholecystectomy, which the physician reported as routine, and the patient was released the same day. However, the patient continued to suffer pain, nausea, and vomiting. It was subsequently determined that the patient suffered from a bile leak, which was corrected by a second surgery.

The patient brought a medical malpractice action against the initial physician and his medical group. A jury determined that the physician was not negligent, and that the injury was instead a result of the patient's unusual anatomy. A state appellate court affirmed the decision, finding that it was not against the manifest weight of the evidence.

Background: In 2012 and the beginning of 2013, a woman suffered from intermittent abdominal pain. The characteristics of her symptoms indicated a likelihood of gallbladder disease. The patient was diagnosed with abnormal functioning gallbladder, which required removal. The general surgeon examined the patient, asked her for a history of her symptoms, and explained the risks and benefits of a cholecystectomy.

The day after the examination, the physician performed a laparoscopic cholecystectomy on the patient. According to the physician, the procedure was seemingly routine, and the patient was released the same day. Nevertheless, the patient was readmitted to the hospital the next day because she was experiencing left-sided chest pain, nausea, and vomiting. She was released a few days thereafter.

Over the next few months, the patient continued to experience intermittent pain and returned to the hospital several times. Ultimately, a bile leak was determined to be the cause of her complications, and she then underwent a second surgery to drain the leak. The leak was caused by an injury that occurred during the first surgery. Despite the second surgery, the patient alleged that she continued to experience pain.

In 2014, the patient filed a medical malpractice lawsuit against the initial physician and his medical group employer. While there was no doubt that the bile duct had, in fact, been injured by the physician during the first surgery, the question was whether the physician had violated the standard of care in causing the injury. The patient presented multiple expert witnesses who focused on the concept of the "critical view of safety," which was developed in order to avoid injuries during laparoscopic surgeries and involves physicians viewing the surgical field through a telescope prior to commencing the procedure.

After hearing expert testimony from both parties, the jury determined that the physician had not been negligent in performing the surgery and that the injury was caused by the patient's unusual anatomy, which could not be seen through the telescope while performing the presurgery critical view of safety. The patient appealed, arguing that the jury's finding was against the manifest weight of the evidence. However, the state court of appeals affirmed the jury verdict and lower court's decision.

What this means to you: An important lesson from this case is that although a patient may have suffered an unexpected injury, it does not necessarily mean that a physician or care provider was negligent. An injured patient may automatically assume and allege that the physician failed to satisfy the standard of care, but an expert's analysis and a jury's determination are more complicated and nuanced. In this case, the jury determined that the physician's care was appropriate, and the appellate court affirmed this determination.

The appellate court's reasoning focused on the fact that, while the patient's expert witnesses presented convincing evidence, the physician's expert testimony also presented facts that would support a claim in the physician's favor. Consequently, there was at least some evidence in support of the jury's verdict, and it would have been incorrect for the court to find that the decision was against the manifest weight of the evidence.

Experts are crucially important for medical malpractice cases, and often are the deciding factor as to the success or failure of claims and defenses. In this case, the expert opinions on which the decision was formed presented slightly diverging views of what constituted the "critical view of safety."

On the patient's side, the experts detailed how, in a laparoscopic cholecystectomy, the area known as Calot's triangle — defined by the cystic duct, the bottom of the liver where the gallbladder attaches, and the common bile duct — must be clearly identified. All fatty tissue must be carefully moved until these structures are clearly visible. In the event that the patient presents an atypical anatomical structure, the procedure must be delayed and further testing performed to determine the actual anatomy of the patient and gain a clear understanding as to how to proceed. There are several structures that could be damaged in the area, and it is necessary to have a complete and clear view of the ducts prior to clipping and cutting them to remove the gallbladder. The patient argued that the physician breached his duty of care in not obtaining a clear critical view of Calot's triangle prior to proceeding with the surgery.

By contrast, the physician and his expert witnesses alleged that the correct procedure was followed. The physician asserted that the hospital where the procedure was performed is a teaching hospital; thus, medical students were present during the procedure and the physician reviewed the textbook explanation of how to achieve the critical view of safety by demonstrating each step of the procedure.

The physician further testified that the procedure was common and routine, and that in his surgical career, he had never injured a duct. He asserted that he believed that the patient had an aberrant branch of her right hepatic duct close to the cystic artery. This branch was hidden and could not be seen through the telescope even though the area had been appropriately cleaned of excess tissue. Because of this aberration, the duct was inadvertently clipped during the procedure.

A second expert physician also testified in the defendant's favor, stating that the physician had not been negligent and the injury had been caused by the presence of an abnormality that could not be detected through the telescope. Ultimately, when presented with all the conflicting expert testimony, it is up to a jury to evaluate and weigh the expert opinions — and it is thus critical for care providers to choose the right expert.

Injuries to bile ducts during laparoscopic cholecystectomies are not uncommon. They can even occur during open cholecystectomies that are performed if scar tissue or other anomalies prevent the laparoscopic approach. When the bile duct is nicked or lacerated, bile leaks occur. These can be readily diagnosed using contrast media during scanning. What is most important to mitigate adverse results is the assurance of a patient's full understanding of risks posed by the surgery, the alternatives to the recommended procedures and the expectations for recovery time, signs and symptoms of possible complications, and aftercare instructions. Obtaining the patient's informed consent for a procedure and documenting the patient's understanding of the risks and benefits involved before the procedure is performed are of critical importance.

Following the procedure, if the symptoms that led the patient to seek medical attention initially are not relieved, then something may be wrong and care providers have a duty to re-evaluate the patient. Patients who feel that their physicians are concerned about their welfare and willing to spend extra time answering questions and providing clear information are much less likely to be litigious.

The key lesson here is how both the patient and physician presented evidence in support of their positions that could have led a reasonable jury to find in either party's favor. As noted by the appellate court, the patient's allegation that the verdict was against the weight of the evidence was untenable based upon the physician's evidence.

Furthermore, the jury's decision as to whether to believe the physician's expert testimony was not for the appellate court to reconsider, as this determination was properly before the jury and subject to deference by the reviewing court. The scope of the appeal required the court to decide whether a reasonable person could have found in favor of the defendant based on the evidence presented at trial. In this case, the appellate court found that the decision was supported by sufficient evidence to find that it was not against the manifest weight of the evidence. ■

REFERENCE

Decided on Feb. 20, 2019, in the Court of Appeals of Ohio, Case Number 2019-Ohio-602.