HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE SINCE 1979

INSIDE

Relias Media

APRIL 2024 Vol. 46, No. 4; p. 37-48

UVA Health Targets Workplace Violence with Low-Cost Program

By Greg Freeman

The University of Virginia (UVA) Health System in Charlottesville has implemented a workplace violence initiative that improved reporting of violent incidents and decreased injuries.

The effort was prompted by a particularly violent event in 2016 that spanned several floors and caused multiple injuries to both staff and the patient involved, says **Lauren Mathes**, BSN, RN, clinic manager.

"After review of the situation, it came to light that there was some known history with the patient that, had all team members been aware of, we could have mitigated a lot of the injury and been more prepared for that situation with that patient," Mathes explains. "That event specifically is what prompted us to get started."

THE SAVE INITIATIVE SOUGHT TO REDUCE INJURY, REDUCE POTENTIAL HARM TO PATIENTS, AND ALIGN GOALS TO BECOME THE SAFEST PLACE TO PROVIDE CARE.

The patient had a history of seizures. The outpatient neurology team knew he exhibited violent behaviors in his post-seizure state. He was admitted to the hospital that day and had a seizure, followed by violent behaviors that the staff outside of neurology did not anticipate.

UVA Health formed a multidisciplinary task force to assess that event, which led to several rapid interventions in early 2017 related to workplace violence. The Situational

Financial Disclosure: None of the planners or authors for this educational activity have relevant financial relationships to disclose with ineligible companies whose primary business is producing, marketing, selling, re-selling, or distributing healthcare products used by or on patients.

HEALTHCARE RISK MANAGEMENT™

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

GST Registration Number: R128870672

SUBSCRIBER INFORMATION:
(800) 688-2421
ReliasMedia.com

JOINTLY ACCREDITED PROVIDER™
INTERPROFESSIONAL CONTINUING EDUCATION

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

Relias LLC designates this enduring material for a maximum of 1.5 *AMA PRA Category 1 Credits*™. Physicians should claim only credit commensurate with the extent of their participation in the activity.

1.5 ANCC contact hours will be awarded to participants who meet the criteria for successful completion.

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

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

Opinions expressed are not necessarily those of this publication. Mention of products or services does not constitute endorsement. Clinical, legal, tax, and other comments are offered for general guidance only; professional counsel should be sought for specific situations.

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

Awareness Violent Event (SAVE) initiative sought to reduce injury, reduce potential harm to patients, and align goals to become the safest place to provide care. The task force had strong support from leadership, Mathes says.

The SAVE team includes clinicians from multiple disciplines, including behavioral medicine, an employee health injury coordinator, the Behavioral Emergency Response Team (BERT), UVA Health security, the university police department, the Office of Patient Safety, risk management staff, and emergency management leaders.

Incident Shows Problems

A year earlier, UVA Health's organizational goals were updated with a primary target of becoming the safest place to work and receive care, says **Janine Smith**, BSN, RN, the RN clinical program coordinator for team member injury prevention. The 2016 incident kicked that effort into high gear, she says.

As staff tried to de-escalate the situation, the patient traveled to different areas in the hospital and committed violent acts against staff and others in those areas, Smith says. The investigation of the incident revealed that staff in those units did not sufficiently understand how to call for help or protect themselves from the violent patient.

"We learned they didn't know who the right person was to call or what information to tell them. They also didn't know how they could let their colleagues on the unit next door know, or how do we lock down a unit," Smith explains. "How do we lock down a floor or stop the elevators? There were some specific learnings from that situation. If you have a mother and baby unit, there's a potential kidnapping, and you would have a process to lock things

down. But with violence, it was clear we can do this but not when should it be done and [know] what the trigger would be."

Understanding acceptable behavior vs. unacceptable behavior was difficult, and the task force quickly realized that it was important to spot potentially violent patients early so that precautions could be put in place.

To help staff identify patients with a potential for violence, UVA Health created a behavioral flag for the medical record that identifies the patient's past behaviors and what caused them, such as a startle reflex. Much of the work initially included patients with delirium and dementia because violence is part of their disease processes. The goal was to treat those patients with respect and give them the care they needed, but also to keep them and the staff safe.

"We wanted a way to identify them and make sure that everybody's on the same page when caring for these patients, and then that flag would follow them through from unit to unit, as well as if they were in the outpatient clinic," Smith says.

Private Security Guards

UVA Health wanted a structured way for staff to call for help when a patient showed signs of violence or acted out violently. The team developed a script that is taped to many of the hospital phones to assist staff in giving the appropriate information for a timely response. The script guides the caller in conveying what they need, whether the patient is acting out or experiencing a psychotic event, whether a weapon is involved, and other details.

The information conveyed in that call helps hospital security determine what kind of response to send, from additional staff to the BERT team and summoning police.

UVA Health also contracted with a private security firm to monitor some patients at high risk for violence, in some cases posting a guard to always sit outside that patient's room, Smith says. The team also realized that while the behavioral flag in the patient's chart was helpful to clinicians, other staff (i.e., transportation, housekeeping, environmental services, and kitchen staff) would not be alerted because they do not access the chart. To remedy that issue, the team developed a "stop banner" to place over the top of the patient's door, signaling to those staff members that they should stop and check with a nurse before entering the room.

ONE CHALLENGE HAS BEEN THE STAFF'S RELUCTANCE TO LABEL A PATIENT AS POTENTIALLY VIOLENT. UVA HEALTH EMPHASIZES THAT THEY ARE LABELING THE BEHAVIOR, NOT THE PATIENTS THEMSELVES.

The initial task force was turned into a permanent committee that reports to UVA Health's safety and security leadership, with ongoing monitoring and assessment of workplace violence, Mathes says. The committee receives notifications of all the BERT events and can follow up with team members from there to ensure that all events are fully documented. That allows the committee to track and trend data, watching for increased violence or patterns that might suggest a need for work in particular areas, Mathes says. UVA Health also queries team members about their fear for safety during or after the event, tracking that rate as part of their safety metrics.

"We do a lot of training and education with team members, going to staff meeting events, and we meet on a monthly basis as a committee. That has continued to remain a very multidisciplinary group," Mathes notes. "We've been able to set up a website with a link on every desktop computer directly to our website, which has a lot of our tools and resources links to how to obtain private security, how to enter the flags in the chart, and how to use the script for calling for help. There is attrition within staffing, so having those as a quick way to find that right on the desktop has been really helpful for a lot of areas."

Locked Unit Doors

The SAVE effort also prompted a change in locking procedures at the facility. Now, doors leading from one unit to another are locked so that a violent patient cannot roam from one area to another as easily as happened in the 2016 event, Smith says.

One challenge has been the staff's reluctance to label a patient as potentially violent. UVA Health emphasizes that they are labeling the behavior, not the patients themselves. Patients in labor and patients recovering from anesthesia may act violently even though they do not act like that normally, Smith notes, so it

is important to record that behavior in the medical record so that staff can anticipate it next time.

"It might be pain-related, so we want to make sure that we're controlling their pain better next time. It's not labeling the patient as a bad patient; it's a behavior that we need to anticipate and make sure that we're figuring out a way to make them most comfortable. Maybe that anesthesia didn't work well for them," Smith says. "If it's an older child or a patient with autism, is there a different intervention that we need to put in place to make sure that we're caring for them the best to keep them safe, as well as the team members safe? Do we need to include their sister? Or do they need to have their teddy bear?"

Agreeing on a definition for workplace violence also can be the biggest obstacle when starting a workplace violence prevention program, followed by the education necessary to get staff to follow new procedures intended to protect them, Mathes says.

The SAVE efforts have resulted in increased reporting of violent incidents but fewer injuries to staff, Mathes says. "When you first start tracking it, you're not going to have something to benchmark by. But as you continue to talk about this, you might see your rates go up because you are getting buy-in from your team and they start reporting more," she notes. "Don't be surprised by that and you can see it as a sign that you're getting the response you need from staff." ■

SOURCES

- **Lauren Mathes**, BSN, RN, Clinic Manager, University of Virginia Health System, Charlottesville. Email: lem9r@uvahealth.org.
- **Janine Smith**, BSN, RN, RN, Clinical Program Coordinator for Team Member Injury Prevention, University of Virginia Health System, Charlottesville. Email: ms4cf@uvahealth.org.

DOJ Signals Dependence on Whistleblowers for False Claims Act Settlements

The Department of Justice (DOJ) recently reported that settlements and judgments under the False Claims Act (FCA) exceeded $2.68 billion in the fiscal year ending Sept. 30, 2023. The government and whistleblowers were party to 543 settlements and judgments — a record number for a single year.[1]

FCA recoveries now total more than $75 billion since Congress strengthened the act in 1986, and healthcare fraud remained a primary portion of all FCA cases. Whistleblowers continued to play prominent roles in healthcare FCA settlements.

The FCA report details many healthcare fraud settlements that can serve as lessons for risk managers and compliance officers, says **Brett W. Johnson**, PC, partner with Snell & Wilmer in Los Angeles.

"Risk managers and counsel need to do a deep dive into the actual settlement agreements to ensure you're not doing X, Y, and Z, as alleged in those claims. Good programs are bringing together risk managers and their other top people to really ensure that not only are we not doing X, Y, and Z, but we're also not doing any analogy of what X, Y, and Z could be," Johnson explains. "The other thing is to try to get ahead of the whistleblowers. It's obvious there are whistleblowers who are willing to quickly make a claim and then be able to get a significant reward if they're correct."

A good defense is to ensure there are multiple opportunities for a whistleblower to internally object to a program. This significantly undermines the whistleblower if it can be proven that they waited until a program was fully implemented before alleging fraud, Johnson says.

"The great mitigating factor is when we gave you 10 different opportunities to object to what we were doing, and you didn't do it. Instead, you laid in wait until the program went into place, and then raised your objections. If we would have known your perspective on this, we may have taken a different action," he says. "Unfortunately, many people within the healthcare industry have been rewarded significantly for this kind of action, so the healthcare industry needs to address it ahead of time."

But at the same time, healthcare organizations must put robust systems in place to respond to any reports of potential fraud, Johnson notes. Reports from a hotline or any other means must be logged promptly and an investigation should be launched without delay. Someone must be assigned to respond to those reports in a timely fashion. That can be the risk manager or counsel. However, care must be taken in having a non-lawyer investigate the reports.

"A lot of risk managers are not lawyers, and when they're out there doing their investigations or their reviews, that's not necessarily privileged unless done at the direction of a lawyer. We're seeing that more and more in the healthcare industry are hiring independent consultants — especially on the billing side — to review bills, and they do not have that privilege," Johnson says. "The courts have made very clear in different cases that if you're not a lawyer, and this isn't done for purposes of obtaining attorney advice about how to respond to a matter, then it's not going to be privileged."

FCA Claims Could Increase

Without privilege, the government can look at everything that the risk manager or a non-lawyer consultant reviewed, Johnson explains. It can be penny-wise but pound-foolish to avoid using lawyers if the whistleblower complaint turns into a significant matter, he says.

Recent settlements and court rulings have been influenced by that issue, and they may prompt an increase in FCA claims and payouts soon. "I think this recent report is going to be small potatoes compared to what will be reported next year because there's been that groundswell of people waiting to see what happened in the Supreme Court cases," Johnson says. "For the last three or four months, the negotiations have been around 'How are we now going to settle this because I'm not paying several million dollars for discovery.' You're going to see a significant spike in settlements and enforcement recovery for 2024."

Johnson notes that in 2023, the U.S. Supreme Court affirmed in *United States ex rel. Polansky v. Executive Health Resources, Inc.* that the Justice Department properly sought and won dismissal of a whistleblower suit accusing a healthcare organization of violating the FCA by improperly billing Medicare. In that ruling, justices questioned whether the whistleblower provision of the FCA was constitutional.[2]

Given the government's reliance on whistleblowers to pursue FCA claims, the court determining the provision invalid would be a big blow to the DOJ, Johnson says. "If it is resolved over the next five or six years and finally gets back to the Supreme Court on a new case, that is what's going to be devastating to this program because the government has such reliance on the whistleblower protection, as shown by this recent report," he explains. "Nobody's talking about that. That's like reading the tea leaves seven years out, but what happens if the whistleblower goes away?"

If that happens, the DOJ probably will have to rely on outsourcing investigations to contractors, which it already does but not nearly to the extent it relies on whistleblowers, Johnson says. Whatever it takes, the government is likely to find a way to continue pursuing FCA cases even without whistleblowers.

Need to Audit COVID-19 Funds

The government also is still focusing on fraud related to COVID-19 funds. "If you look back at the American Recovery and Reinvestment Act cases back from the Great Recession, some of those cases didn't get resolved for seven [or] eight years after the recession and those programs ended. I see that coming in," Johnson says. "The healthcare industry is going to get a double whammy because they're a target industry anyway, and then they were one of the big recipients of COVID funds."

Johnson recommends getting ahead of those investigations with internal audit programs. In some cases, a healthcare organization may find it was not in compliance with government requirements for the use of COVID-19 funds, but not necessarily with any ill intention.

"The government kept moving the goalposts on some of those programs. They put out guidelines saying, 'Hey, take this money, and this is how you want to use it.' Then, guidelines would come out after the money was already delivered, saying, 'Well, we really want you to use it this way,' or 'This is what we meant by

EXECUTIVE SUMMARY

The healthcare sector continues to dominate the government's settlements related to False Claims Act (FCA) violations. Efforts continue to recover funds improperly used from COVID-19 relief programs.

- The Supreme Court has expressed doubt about the use of whistleblowers in FCA claims.
- Healthcare organizations should conduct internal audits to discover problems before the Department of Justice does.
- Investigations conducted by non-lawyers might not be privileged.

those guidelines,'" Johnson explains. "But the money was already spent. Companies in the healthcare industry are going to have to determine 'What does that really mean? Do I just pay back the money to avoid a False Claims Act case?'"

Johnson notes that FCA settlements can be more common in healthcare than in other industries, like military suppliers. An FCA claim can affect licenses and the ability to provide healthcare, so the reported numbers on FCA claims can seem disproportionately large in the healthcare industry.

"It's not because the healthcare industry is worse or did worse things than the other industries. They just have more to lose," Johnson says. "When you combine that with the significant costs associated with discovery, they do the math and they say, 'This can impact our licenses. This is going to cost us millions to defend even though we didn't do anything wrong, so we have to settle.'" ■

REFERENCES

1. U.S. Department of Justice. False Claims Act settlements and judgments exceed $2.68 billion in fiscal year 2023. Feb. 22, 2024. https://www.justice.gov/opa/pr/false-claims-act-settlements-and-judgments-exceed-268-billion-fiscal-year-2023
2. *United States ex rel. Polansky v. Executive Health Resources, Inc.* June 16, 2023. https://www.supremecourt.gov/opinions/22pdf/21-1052_fd9g.pdf

SOURCE

- **Brett W. Johnson**, JD, Partner, Snell & Wilmer, Los Angeles. Phone: (602) 382-6312. Email: bwjohnson@swlaw.com.

Patient and Family Complaints Require Careful Response

Complaints from patients or family members are commonplace in healthcare, but knowing how to respond is not always clear. Some complaints will be trivial or unfounded, while others may indicate a serious patient safety issue or an incident that could lead to litigation and liability.

Risk managers can help channel those complaints in the right direction by helping frontline staff know how to respond, as well as when and when not to escalate the complaint.

There is no magic answer to what to say in response to a complaint, says **Paul D. Werner**, JD, an attorney with Buttaci Leardi & Werner in Tarrytown, NY. It is impossible to predict how the complainant will react to anything because the situation often is quite charged and dynamic.

"While it can be frustrating to not have a script when addressing complaints, the lack of a specific methodology also gives those responding to the complaint the ability to adapt to the specific circumstances," Werner says. "Anyone who may potentially be responding to a complaint in the healthcare context should be trained on the basic do's and don'ts, but also trained on substantive matters that will afford them the ability to review and react to the situation."

Werner advises clients to avoid making concessions or direct apologies for actions or behaviors and instead focus on understanding and empathizing with the complainant's situation. For example, rather than directly conceding that an error was made when talking with a complainant, Werner often advises clients to apologize for the inconvenience the complainant perceives or the problem the complainant is mentioning.

"By way of a specific example, I advise clients to say, 'I'm sorry to hear that you're experiencing discomfort,' or 'I'm sorry you're surprised by the fact that you were billed for that

EXECUTIVE SUMMARY

Healthcare organizations should have processes for responding to complaints from patients and families. The nature and seriousness of the complaint will dictate how much of a response is required.

- Clinicians and other staff should be trained in the proper response to complaints.
- Always be courteous and nonconfrontational when responding.
- Some complaints should be escalated to risk management for further investigation.

service,' as opposed to 'I'm sorry that happened to you,' or 'I'm sorry for that error.'" Werner explains.

Documentation Is Key

Any complaint should be fully documented in the patient's chart. To the extent a complaint is received in writing, that writing should be preserved in the file as well. Any audio or video recordings of the complaint, if they exist, also should be preserved.

In addition to documenting the complaint, any actions taken in response to the complaint should be documented, Werner says. If an internal investigation is conducted, that should be done with the assistance of counsel to ensure completeness and to protect privilege.

Lend a Sympathetic Ear

There should not be much difference in how clinicians and administrators respond, Werner says. Because clinicians are much more likely to receive complaints in person with the complainant face-to-face, clinicians need to maintain composure and provide thoughtful, calculated responses.

When hearing a complaint in person, it is recommended that the clinician simply listen to the complaint, acknowledge that it has been made, and assure the complainant that they will investigate and respond, Werner advises. Off-the-cuff responses, especially when there is the potential that professional judgment or skill is being questioned, often escalate things unnecessarily.

"The best tool in the toolbox for de-escalating a situation is being sure to listen to complaints, not simply hear them. Listening to and understanding the complaint allows you to provide a more thoughtful and complete response," Werner says. "In my experience, when the first response to the complaint is insufficient or perceived as a 'blow-off,' complainants are much more likely to press on."

Healthcare professionals should be receptive, empathetic, and sympathetic to anyone who is complaining, says **Eric S. Strober**, JD, partner with Rivkin Radler in New York City. It is normal for patients and families to want everything to go perfectly right every single time, and healthcare workers know that is not reality, he notes. That may lead to frustration with a complaint that seems unrealistic, but healthcare staff should nonetheless respond in an understanding way.

"If you address it and sympathize with the complainer's point of view and try to make sure that there's no harm done, then that's the best you can do under those circumstances. I don't think being defensive and knee-jerk reactions are the best way to go," Strober says. "You're not going to calm anybody down or assuage any kind of concerns by getting immediately defensive. In fact, you could just inflame matters that way."

Not every complaint needs to be escalated to risk management or nursing administration, but some do, Strober notes. A complaint about the response time for calling in a prescription or how long a patient had to sit in a room is just a garden-variety dissatisfaction with the realities of medical care in America in 2024.

"Those don't need to be reported to risk management. If there's no adverse event and no injury or no harm that has come to a patient, then it doesn't seem like there's a need to report anything," Strober says. "But if somebody was inadvertently stuck with a needle while someone was trying to draw blood — sure, report that."

Streamline the Response Process

Providers should have a streamlined process for responding to patient complaints, says **Aubrey B. Gulledge**, JD, an attorney with Baker Donelson in Memphis, TN. All complaints that rise to a level of severity to pose a threat of litigation or a threat to safety should be directed to risk management as soon as possible. The complaint should be acknowledged in a timely and conciliatory fashion, and the response should reflect that the provider takes the complaint seriously and is investigating.

Clinicians and administrators should consider that written communications with patients and their families are discoverable in litigation, Gulledge notes. Any complaint response should not include overreaching promises of remedial action, legalese, or medical jargon.

"Providers should be cognizant of privacy and confidentiality concerns when responding to complaints, and responses should not reference specific individuals," she says. "Providers should never comment regarding whether there was any lack of compliance with the standard of care applicable to the provider, or whether there was a perceived lack of compliance with policy or regulations. The responses should avoid commentary that could expand the facts involved in the complaint."

Risk management should have a process for documenting patient

complaints that includes the date of the complaint, the name of the person complaining and/or patient name, indication of who received the complaint, the content of the complaint, an indication of whether the complaint was written or verbal, and recommended follow-up, Gulledge says.

Gulledge notes that the necessary action depends on the nature of the complaint and the potential effect on the patient, other patients, and the public. When patient safety is at issue, engaging all stakeholders to take appropriate immediate action is imperative.

Follow-up communication with the patient and/or family should always happen, and in severe instances, risk management should be aware of potential third-party investigation, she says. The follow-up should acknowledge receipt of the complaint, and should occur upon completion of the investigation.

Both clinicians and administrators should engage their legal representatives and risk management professionals when they become aware of a patient complaint that involves patient safety issues and/or could turn into litigation, Gulledge advises. Clinicians should indicate that they have forwarded the complaint to management. Clinicians who are not in management positions should proceed with the direction of management and/or legal according to the department's policies and procedures. They should document in the medical record if they have personally received a complaint but should not document any communications with risk management or discussions regarding remedial action.

"We often find that the reason for litigation is the lack of understanding of what happened to the patient. Clinicians who take the time to explain disease processes and answer questions when there is an unexpected outcome are less likely to be sued," Gulledge says. "Taking time with patients and family members and not appearing to be in a hurry or cut them off when they ask questions will help avoid litigation."

Prompt and frequent communication with the patient or family is the most critical component of attempting de-escalation, Gulledge notes. A written record of acknowledgment, investigation, response, and follow-up is a powerful tool in ensuring a comprehensive response to complaints and best efforts to avoid future litigation. "This communication is the best way to promote patient satisfaction and gain, maintain, or regain patient and family trust," she says.

Do Not Admit Wrongdoing

From the perspective of litigation and complaints of medical incidents that have resulted in harm, the first step in responding to a complaint is to take it seriously and to show appropriate empathy without admitting to any wrongdoing, says **Bill Bower**, senior vice president with Gallagher Bassett in Rolling Meadows, IL, which provides healthcare professional liability claims and risk management consulting. Previously, Bower was chief risk officer at a major health system. Patients and family members should be advised that their complaint will be investigated, and that the institution will get back to them.

Many organizations have a disclosure policy or protocol that dictates the methods by which the institution will respond, Bower notes. Internally, complaints should be directed to the risk management department or to the particular body within the organization that is charged with clinical investigations of incidents. Often, this will allow for a determination of whether the complaint arises from an incident that might provide an opportunity for process improvement. This will lead to routing to the appropriate team — perhaps risk, patient safety, or process improvement. In addition, a complaint should be directed to those within the organization who are charged with notifying insurers of events that could result in a claim.

"If there are artifacts or evidence involved in the event — video coverage, retained foreign bodies, pathology, etc. — it is essential that such evidence be preserved. If an investigation reveals further evidence, such as text messages, these must also be preserved," Bower says. "Oftentimes, if the event is of a certain magnitude or litigation seems likely from the start, retention of counsel can be employed to begin an analysis from that perspective and to gain attorney-client privilege where feasible. Privilege may also be afforded under the Patient Safety Act as patient safety work product, if applicable." ■

SOURCES

- **Bill Bower**, Senior Vice President, Gallagher Bassett, Rolling Meadows, IL. Phone: (630) 773-3800.
- **Aubrey B. Gulledge**, JD, Baker Donelson. Memphis, TN. Phone: (901) 577-2218. Email: agulledge@bakerdonelson.com.
- **Eric S. Strober**, JD, Partner, Rivkin Radler, New York City. Phone: (212) 455-9560. Email: eric.strober@rivkin.com.
- **Paul D. Werner**, JD, Buttaci Leardi & Werner, Tarrytown, NY. Phone: (609)799-5150. Email: pdwerner@buttacilaw.com.

HHS Proposes Cybersecurity Requirements for Hospitals

The Department of Health and Human Services (HHS) recently released a concept paper outlining its cybersecurity strategy for the healthcare sector, focusing specifically on strengthening resilience for hospitals threatened by cyberattacks. HHS outlined four pillars for action, including new voluntary healthcare-specific cybersecurity performance goals.[1]

Cyber incidents in healthcare are increasing. HHS reported a 93% increase in large breaches reported to the Office for Civil Rights (OCR) from 2018 to 2022 — from 369 incidents to 712. There was a 278% increase in large breaches involving ransomware.[2]

"The healthcare sector is experiencing a significant rise in cyberattacks, putting patient safety at risk. These attacks expose vulnerabilities in our healthcare system, degrade patient trust, and ultimately endanger patient safety," said HHS Deputy Secretary **Andrea Palm**. "HHS takes these threats very seriously, and we are taking steps that will ensure our hospitals, patients, and communities impacted by cyberattacks are better prepared and more secure."[2]

The HHS concept paper outlines these initiatives:

- **"Publish voluntary Healthcare and Public Health sector Cybersecurity Performance Goals (HPH CPGs).** HHS will release HPH CPGs to help healthcare institutions plan and prioritize implementation of high-impact cybersecurity practices."
- **"Provide resources to incentivize and implement cybersecurity practices.** HHS will work with Congress to obtain new authority and funding to administer financial support and incentives for domestic hospitals to implement high-impact cybersecurity practices."
- **"Implement an HHS-wide strategy to support greater enforcement and accountability.** HHS will propose new enforceable cybersecurity standards, informed by the HPH CPGs, that would be incorporated into existing programs, including Medicare and Medicaid and the HIPAA Security Rule."
- **"Expand and mature the one-stop shop within HHS for healthcare sector cybersecurity.** HHS will mature the Administration for Strategic Preparedness and Response's coordination role as a 'one-stop shop' for healthcare cybersecurity which will improve coordination within HHS and the federal government, deepen HHS and the federal government's partnership with industry, improve access and uptake of government support and services, and increase HHS's incident response capabilities."

More Regulatory Issues Could Emerge

Hospitals are grappling with unprecedented levels of cybersecurity issues and might welcome a higher level of regulation, says **Jolie Apicella**, JD, partner with Wiggin and Dana in New York City. However, that could come with new, emerging legal and regulatory issues on top of the regulations that they already face.

"HHS's mission here is to improve overall cybersecurity practices and build up the resiliency of the programs. These cybersecurity threats are really criminal operations, so hospitals have to now implement the absolute best cybersecurity practices. Not only that, but they have to live up to them, which is a very difficult thing to do," Apicella explains. "There could just be a slip-up, there might not even be any exposure or any sort of leaks that come from that, but they can then be on the hook."

The concept paper tells healthcare organizations where HHS is setting its priorities. "They're definitely working as hard as they can to improve the overall cybersecurity practices of hospitals because they are some of the most vulnerable targets," Apicella says. "They want to publicize any vulnerability that the hospitals may have as a way for the public to feel comfort that the hospital would be held accountable."

The concept paper draws attention to OCR's recently updated telehealth

EXECUTIVE SUMMARY

A concept paper from the Department of Health and Human Services (HHS) provides a cybersecurity strategy for healthcare organizations. The voluntary goals could become requirements soon.

- Cybersecurity incidents continue to increase every year.
- HHS will establish voluntary cybersecurity performance goals.
- Telehealth disclosure is noted in the paper as a particular concern.

guidance, notes **Jason Johnson**, JD, partner with Crowell & Moring in New York City. Along with guidance from the Federal Trade Commission, the HHS concept paper signals a joint collaborative effort that health organizations should heed.

"For telehealth, this is really the first significant paper that's put together a bunch of items on the telehealth side to provide some concrete information as to the use and access of telehealth," Johnson says. "During COVID, there was discretion from OCR around enforcement, and now we've kind of moved into the next phase where entities need to pay attention to what OCR is saying about this."

A key concern should be ensuring that the organization provides full disclosure to individuals, Johnson says. "It's important that your patients understand the privacy and security protections in place, and the risks that go along with that. I think that's a little bit of a significant deviation from what we've seen in the past," he notes. "This puts the burden on these entities to provide additional information and disclosure to those individuals that is in line with what you see outside of healthcare. I don't think a lot of healthcare entities probably are very well versed on that."

Voluntary Could Become Mandatory

The cyber performance goals to be developed by HHS would be voluntary at first but may become requirements soon, says **Kirsten Mickelson**, cyber practice group leader with Gallagher Bassett in Rolling Meadows, IL, which provides healthcare professional liability claims and risk management consulting.

"There are references in the proposal which are signaling that they will become requirements as early as this year. It builds on the Biden administration's national security strategy and serves as an introduction to HHS's own cybersecurity strategy," Mickelson explains. "I think it's significant because it offers insight to the healthcare sector into the more active role HHS will probably play in the cybersecurity space."

Through Sector Risk Management Agencies, HHS would be responsible for sharing cyber threat information and intelligence with the healthcare sector, but then also provide technical assistance, guidance, and resources to comply with the data security and privacy laws.

"This is coming from the highest level," Mickelson says. "It is significant in that sense because it demonstrates the level of involvement HHS will have with the government and the current administration in terms of sharing the threat intelligence. It shows that the overall goal is driving enhancements to critical infrastructure security."

HHS is signaling that they are holding healthcare organizations responsible for breaches, says **William P. Dillon**, JD, shareholder with Gunster law firm in Tallahassee, FL. Regulators may have had more sympathy in the past because organizations were up against sophisticated hackers with quickly emerging technology, he says.

"Then, they looked and said they failed to conduct a risk analysis, they didn't have policies or procedures in place to regularly review information system activity. They're pushing the same thing that they've been saying for years, and if people aren't adhering to that, I think OCR is taking the position of saying, 'We're going to have to do a two-pronged approach,'" Dillon says. "They're continuing to do education, but now they're holding some people's feet to the fire."

The cybersecurity plan does not seem to address one key failing in the government's enforcement of existing requirements, says **Iliana L. Peters**, JD, shareholder with Polsinelli in Washington, DC. Previously, Peters was acting deputy director for HHS and enforced HIPAA regulations. HHS responds vigorously to self-reported cyber breaches but does little to audit compliance and find unreported incidents, she says.

"All I see — at least for now, and I'm hoping that that will change — is increased enforcement against those entities who are doing something right. They're not doing everything right, but they have compliance programs and they're reporting breaches," Peters says. "Some of the enhanced goals are already required by law, so I'm a little confused about how that is an enhanced goal when it is something that arguably they should already be doing."

With the increased risk of cyber threats, cyber insurance is much harder to get now, and the insurers want to see more proof that the organization is taking adequate steps to protect against attacks, Peters says.

"You have to be investing money into understanding what your risk landscape looks like. That is risk analysis, risk management, implementation of really good controls, technical controls, data loss prevention, multifactor authentication — all of those things," she says. "You're never done with cybersecurity preparedness because the threats are constantly changing." ■

REFERENCES

1. U.S. Department of Health and Human Services. *Healthcare Sector*

Cybersecurity: Introduction to the Strategy of the U.S. Department of Health and Human Services. December 2023. https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf
2. U.S. Department of Health and Human Services. HHS announces next steps in ongoing work to enhance cybersecurity for health care and public health sectors. Dec. 6, 2023. https://www.hhs.gov/about/news/2023/12/06/hhs-announces-next-steps-ongoing-work-enhance-cybersecurity-health-care-public-health-sectors.html

SOURCES

- **Jolie Apicella**, JD, Partner, Wiggin and Dana, New York City. Phone: (212) 551-2844. Email: japicella@wiggin.com.
- **William P. Dillon**, JD, Shareholder, Gunster, Tallahassee, FL. Phone: (850) 521-1708. Email: wdillon@gunster.com.
- **Jason Johnson**, JD, Partner, Crowell & Moring, New York City. Phone: (212) 520-1860. Email: jjohnson@crowell.com.
- **Kirsten Mickelson**, Cyber Practice Group Leader, Gallagher Bassett, Rolling Meadows, IL. Phone: (630) 773-3800.
- **Iliana L. Peters**, JD, Shareholder, Polsinelli, Washington, DC. Phone: (202) 626-8327. Email: ipeters@polsinelli.com.

Hospital Crippled by Days-Long Cyberattack

Lurie Children's Hospital, Chicago's largest pediatric provider, experienced a cyberattack that crippled its email systems and most of its phone service for nearly two weeks. The hospital's Epic MyChart system remained offline after most services were restored, requiring patients, families, and community providers to instead use a call center the hospital launched after the attack.

The Rhysida ransomware group reportedly claimed responsibility for the cyberattack and listed the hospital's data for sale on a dark web site for $3.4 million, but the hospital did not confirm those reports.[1]

The Chicago incident highlights the need for healthcare organizations to take steps that can mitigate risk up front before something goes wrong, says **Donald DePass**, JD, an attorney with Hogan Lovells in Washington, DC. Organizations can enforce data minimization and retention practices that limit the information they maintain that could be exposed in an incident, he says. That includes limiting the amount of personal information collected to what is necessary for them to provide their products and services to their customers and their patients.

"The idea is restricting the footprint and limiting the number of places that the data resides and potentially could be subject to unauthorized access or use," DePass says. "Another step organizations can take to mitigate risk up front is just educating their workforces on the protections that they have in place to safeguard data [and] training on privacy and security policies."

It also is important to promptly apply software updates and patches, use tools like multifactor authentication and encryption, regularly back up important data, and regularly evaluate the effectiveness of security controls to identify potential risks and vulnerabilities, DePass says.

"Organizations would be wise to make sure that their vendors are taking similar actions. Often, when a healthcare organization experiences an incident that impacts its data, the incident actually originates from a vendor or service provider that they've entrusted with their sensitive data," he says. "It would be prudent to confirm that those vendors are also taking appropriate actions to protect the data." ■

REFERENCE

1. Gallardo M. Lurie Children's Hospital restores key systems more than month after cyberattack. ABC7 Chicago. March 5, 2024. https://abc7chicago.com/lurie-childrens-hospital-chicago-new-my-chart-cyberattack/14492465/

SOURCE

- **Donald DePass**, JD, Hogan Lovells, Washington, DC. Phone: (202) 637-3286. Email: donald.depass@hoganlovells.com.

COMING IN FUTURE MONTHS

- Trends in medical malpractice claims
- Addressing compassion fatigue
- Hot topics in compliance
- Are HIPAA audits returning?

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 test with a score of 80%; you will be allowed to answer the questions as many times as needed to achieve a score of 80%.

4. After successfully completing the test, your browser will be automatically directed to the activity evaluation form, which you will submit online.

5. Once the completed evaluation is received, a credit letter will be emailed to you.

CME/CE QUESTIONS

1. **What prompted the violent outburst by a patient during the 2016 incident at the University of Virginia (UVA) Health System in Charlottesville?**

   a. A seizure
   b. A drug overdose
   c. An escape from police custody
   d. A reaction to anesthesia

2. **When the UVA Health team realized the medical chart flag did not alert nonclinicians to the presence of a potentially violent patient, what solution did they implement?**

   a. Nurses verbally spread the word to nonclinician staff such as housekeepers.
   b. A "stop banner" was placed over the top of the patient's door to alert those staff.
   c. Nurses took over housekeeping and meal delivery for those patients.
   d. Housekeeping and food delivery were delayed until a security guard could be present.

3. **What does Paul D. Werner, JD, advise regarding responding to complaints?**

   a. Always begin by apologizing.
   b. Avoid making concessions or direct apologies for actions or behaviors.
   c. Document the complaint in writing and ask the person to sign it.
   d. Pass even the smallest complaints to risk management for evaluation.

4. **The Department of Health and Human Services reported that from 2018-2022, there has been how much of an increase in large breaches reported to the Office for Civil Rights?**

   a. 23%
   b. 53%
   c. 73%
   d. 93%

CME/CE OBJECTIVES

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

- Describe the legal, clinical, financial, and managerial issues pertinent to risk management.
- Explain the impact of risk management issues on patients, physicians, nurses, legal counsel, and management.
- Identify solutions to risk management problems in healthcare for hospital personnel to use in overcoming the challenges they encounter in daily practice.

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

Failure to Diagnose and Treat Post-Surgery Infection Leads to $1.18 Million Verdict

*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

News: A woman underwent surgery on her wrist with no initial reported complications. She was instructed not to soak her hand until after the sutures were removed. The patient reported multiple symptoms, including pain, redness, and swelling. She had multiple follow-up visits, but the surgeon failed to diagnose or treat an infection. After visiting a different facility, the patient was diagnosed and treated, but the delay caused significant loss of function to her hand.

The patient sued, alleging that the delay and lack of treatment constituted malpractice. The defendant providers denied liability and claimed that the patient initially reported (but then denied) soaking her hand. A jury agreed with the patient and awarded $1.18 million, which was upheld on appeal.

Background: On Jan. 7, 2016, a woman underwent surgery on her right wrist as a treatment for carpal tunnel syndrome. There were no reported complications during the surgery, and the patient was discharged from the hospital the same day. Before discharge, the surgeon instructed the patient to return in 10 days for suture removal. The surgeon also told the patient not to soak her hand in water, which would reduce the risk of infection. A nurse provided written discharge instructions that stated, "Keep hand clean and dry until sutures removed; no soaking hand in water."

Within three or four days, the patient reported that her wrist felt "warm" to the touch, and the incision area was red. The patient contacted the surgeon's office and spoke to the medical assistant, but no action was taken. The patient called the surgeon's office multiple times, asking for more or different pain medications, which were refused. The medical assistant did not record a note for each call but claimed to have discussed each call with the surgeon. The medical assistant claimed that the patient never reported that the wound was red, hot, foul-smelling, swollen, or any other circumstances that would have suggested an infection.

THE PATIENT CONTINUED TO REPORT PAIN, SWELLING, AND REDNESS, NOTED THAT HER WRIST BEGAN TO OOZE AT THE INCISION LOCATION, AND REPORTED AN ODD SMELL.

Approximately seven to 10 days after the surgery, the patient returned for suture removal. The surgeon's medical assistant removed the patient's sutures and noted that the wound was not infected or swollen. The surgeon's physician assistant also examined the patient and did not find any remaining sutures, nor did she see any infection or redness. One day later, the patient called and asked to see the surgeon, but she was denied because the medical assistant said the patient's wrist was "fine."

The patient continued to report pain, swelling, and redness, noted that her wrist began to ooze at the incision location, and reported an odd smell. The patient called several times, but no follow-up visit was scheduled. The medical assistant claimed that the patient never mentioned redness or pain symptoms after the sutures were removed, and if the patient had reported such symptoms,

the medical assistant would have immediately brought the patient in and told the surgeon.

On Jan. 22, the patient went to an emergency department (ED) seeking treatment for pain in her wrists. ED physicians diagnosed the patient with an infection, prescribed antibiotics, and told her to schedule an appointment with the surgeon. On Jan. 25, the patient spoke to the surgeon's office and made a follow-up appointment for the next day. At that appointment, the surgeon recommended immediate surgery to treat the infection. A note dated Jan. 26 claimed that the suture removal was unremarkable, did not note any problems, and listed that the patient noted she had been soaking her hand at home. However, the patient subsequently denied soaking her hand after the surgery.

On Jan. 26, the patient underwent surgery to treat the infection. She remained in the hospital for 11 days, during which she underwent two additional surgeries. The patient eventually recovered but lost significant use of her right hand. The patient filed a malpractice suit against the surgeon, the medical assistant, and their practice group. The patient argued that the delay in diagnosing her infection resulted in significant progression of the infection, requiring three additional surgeries and an 11-day hospital stay. The defendants denied liability, and two experts testified that the patient's hand-soaking caused or increased the severity of the infection. However, neither expert could pinpoint when the soaking occurred.

After a four-day trial, the jury awarded the patient damages of $1.18 million. The defendants appealed, arguing that the trial court erred by failing to instruct the jury that the patient contributed to her injury. The appellate court upheld the ruling, noting insufficient evidence that the patient failed to mitigate her damages.

What this means to you: One of the primary takeaways from this case is the importance of keeping thorough and accurate records. A significant issue occurred when the patient allegedly soaked her hand. While the patient denied soaking her hand at all, the defendants' records noted that the patient had been soaking her hand at home. However, the records did not indicate when that alleged soaking occurred — and it made a crucial difference as to whether the patient was partially at fault. If the patient had soaked her hand before the sutures were removed, then she violated the instructions provided by the surgeon after the surgery. Alternatively, if the patient soaked her hand after the sutures were removed, then it would be unproblematic.

Unfortunately for the defendants, the timeline was unclear as to whether the patient soaked before or after suture removal. The records merely indicated that she "had been soaking her hand," without specifying when. Based on the multiple visits, this ambiguity led the court and jury to conclude that the patient may not have been responsible for causing or exacerbating her injury. The defendants made this argument and presented two experts who testified that the patient's hand-soaking would have caused or exacerbated an infection.

This ambiguity would have been resolved had the care providers simply asked the patient "When did you soak your hand?" after she reported soaking. Ultimately, it still might have been an unfavorable result for the providers if the patient had soaked it after the suture removal, but that nevertheless would have enabled the defendants to better understand and consider their prospective liability.

Keeping thorough and accurate records also is important given the length of time that lapses between the underlying medical services and the potential for legal action, particularly trials. The patient's surgery occurred in January 2016, with the trial proceeding years after that. Memories inherently fade, and whether a patient claimed to take an action or not may be determinative to the case, yet difficult to prove. Here, the patient denied reporting that she soaked her hand, while the medical records contradicted that. Providers who keep contemporaneous records that are consistently thorough and accurate will have a better time arguing to a court or jury that their version of the events, as confirmed by the written records, is the correct version of events. On the other hand, providers who do not keep records or who keep sparse, vague records do not have the advantage of referring to contemporaneous documents from years ago.

Here, the surgeon vaguely listed that the patient soaked her hand but did not list when, which resulted in the jury finding insufficient evidence to support the defendants' argument that the infection was caused or exacerbated by the soaking. The appellate court recognized that even the facts most favorable to the defendants did not show that the patient failed to mitigate her injuries, or how the supposed hand-soaking exacerbated the patient's injuries. It is easy to contemplate how a single question posed to the patient, with the response included in the medical records, could have flipped this entire case: The defendants could have demonstrated that the patient defied their instructions, caused, or aggravated her injury, and thus she was at fault. Alternatively, the defendants could have recognized the lack of sufficiency sooner by

knowing that the patient soaked it after the suture removal and could have pushed to settle the case for a substantially lower figure.

Finally, it is important to note that the patient was only communicating with the medical assistant in the initial postoperative period. A medical assistant cannot assess a patient's needs, diagnose an infection (or lack of one), order treatment, document symptoms in the medical record, or provide any intervention except to communicate data to the attending physician or equally qualified designee. Physicians need to rely on paraprofessional assistants who are qualified and licensed by state and federal agencies after significant and appropriate training. A second issue involves the continuing complaints of pain and swelling that were not resolving as expected. If the postoperative course is not following the expected path, there often is a reason that must be investigated. It is always prudent for the physician to make time to look at and listen to patients and not assume anything until they do. Paying attention to expected outcomes is only going to benefit both the patient and physician if the physician pays even more attention to the unexpected outcome. ■

REFERENCE

- Decided Jan. 30, 2024, in the Court of Appeals of Virginia, Case Number 1521-22-1.

Defendants Prevail Against Malpractice Claims Related to Hernia Surgery and Medication List

News: A man underwent successful hernia surgery. However, the next day, the patient suffered what he alleged to be a postoperative respiratory arrest. The patient blamed multiple care providers: the surgeon, the anesthesiologist, the hospital, and his primary care physician (PCP). Each defendant denied liability.

A trial court agreed that neither the surgeon nor the anesthesiologist committed malpractice and dismissed them before trial. A jury found that neither the hospital nor the PCP committed malpractice. The patient appealed, claiming that the jury erred in weighing the evidence and that the remaining defendants erroneously blamed the dismissed defendants. An appellate court rejected that argument and affirmed the verdict for the defendants.

Background: On July 27, 2015, a man underwent a hernia surgery. The surgery was performed without issue. Afterward, the patient's wife and other family members reported the patient struggled to breathe. The following day, the patient suffered a postoperative respiratory arrest.

According to the patient, his PCP failed to list certain medications that the patient was taking for a respiratory condition on a presurgical clearance form that was forwarded to the hospital. Because of this, the hospital was unaware that the patient needed the medication to breathe, to prevent respiratory arrest, and to prevent coma.

The patient and his wife sued the hospital, the surgeon, the anesthesiologist, and the patient's PCP. Before trial, the surgeon and the anesthesiologist filed motions for summary judgment, arguing that the evidence showed they adhered to the applicable standards of care and committed no malpractice. The trial court granted those motions and dismissed both care providers from the case. The matter proceeded to trial against the hospital and the patient's PCP.

Both the hospital and PCP defended during the trial. The PCP admitted that she should have listed his medications but did not. However, the PCP defended on the basis that the physicians at the hospital were aware that the patient was taking those medications because they were documented in a medication list contained in the hospital chart. Moreover, the surgeon and the anesthesiologist had records listing the patient's respiratory condition and medications. Additionally, the patient alleged that the hospital staff failed to appropriately respond to complaints by the patient's family members that the patient was struggling to breathe.

During the trial, the patient's experts testified that the hospital nurse's failure to respond to his breathing complaints was a substantial factor in causing his respiratory arrest. Finally, the defendants argued that the patient was not in respiratory distress, but instead suffered a transient arrhythmia that was unrelated to the failure to take his medication. The defendants' expert testified that other factors, including the patient's obesity and long-term hypertension, contributed to the sudden rhythm disturbance of his heart.

The jury found that although the PCP departed from the applicable

standards of care, the departure was not a substantial factor in causing the patient's injuries. They also found that the hospital did not depart from the applicable standards of care. The patient appealed, arguing that the verdict was contrary to the weight of the evidence, and requested a new trial. He also argued that the remaining defendants — the hospital and PCP — attempted to deflect blame on the two dismissed defendants — the surgeon and anesthesiologist. The appellate court affirmed the verdict, ruling that the evidence supported the verdict and no error occurred. The court noted no shifting of blame to the dismissed defendants; the remaining defendants were permitted to discuss those care providers' records and actions even though they had been dismissed.

What this means to you: This case has many lessons to learn from the multiple defendants, multiple theories of malpractice liability, and multiple defenses. Perhaps one of the more interesting aspects of this case relates to the patient's PCP, who was one of the two remaining defendants when the matter proceeded to trial. The PCP admitted that she did not include the patient's respiratory medications on the list — and the jury ultimately found that this was a departure from the applicable standard of care. Fortunately for the PCP, liability for medical malpractice requires more than a deviation from the applicable standard of care — the patient must suffer injury because of that deviation.

Here, the PCP argued that the patient's injuries were not caused by her failure to note the medication on the requested list. This argument was supported by substantial written evidence, including the hospital's and anesthesiologist's records. Those records confirmed that the other care providers knew about the patient's respiratory condition and that he was supposed to be taking certain medications. The PCP alleged that although she neglected to include the medication in the list, others knew about it anyway, so her shortcoming was inconsequential. The jury agreed with the PCP, finding that her departure was not a substantial factor in the patient's injuries.

THIS CASE HAS MANY LESSONS TO LEARN FROM THE MULTIPLE DEFENDANTS, MULTIPLE THEORIES OF MALPRACTICE LIABILITY, AND MULTIPLE DEFENSES.

Moreover, both defendants presented expert testimony that the patient's injury the day after his surgery was not caused by the medication issue. When there is an alternate cause, as here with the patient's other contributing factors, a provider's failure to adhere to the applicable standard of care may not be the substantial cause of the injury. The outcome of this case could have been different with another patient who had no other contributing factors, but here, the PCP and hospital proffered viable alternatives as to the cause of the patient's injuries. Causation is a necessary element for medical malpractice, and this case offers insight into multiple methods for challenging a patient's allegations of causation.

Even if a provider unquestionably fell below the standard of care, that does not automatically implicate malpractice liability. In defending against allegations of malpractice, it may be wise for providers to choose their battles. Acknowledging wrongdoing may garner the jury's favor, and then the provider can attack the patient's case by challenging a different element. Providers should consider with counsel how to capitalize on what would otherwise be damaging evidence. Here, if the PCP had denied that she failed to provide the medication on the list, it could have resulted in lost credibility, harming her case. Instead, she admitted her mistake and successfully defeated the patient's case on causation.

Finally, note that medication reconciliation has been a standard of patient care for all providers and patients for some time. The patient has the responsibility to provide caregivers with a list of all medications taken at home, including vitamins, supplements, topicals, and anything else prescribed or over the counter. In turn, providers must update that list as changes occur and communicate those changes to patients and their families. Other providers, such as physician assistants and nurses, must review medication lists with patients on admission to healthcare facilities, at clinic or physician office visits, home visits, and any other encounter, including outpatient visits to surgery centers. These practices help avoid errors made by caregivers and harm suffered by patients who were not offered their routine medications in a healthcare setting outside of their own homes. ■

REFERENCE

- Decided Feb. 21, 2024, in the Supreme Court of the State of New York Appellate Division: Second Judicial Department, Case Number 702055/2017.