HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE SINCE 1979

INSIDE

Relias Media

From **Relias**

JANUARY 2022 Vol. 44, No. 1; p. 1-12

Evidence Shows Apology Laws Are Largely Ineffective

What was once a nagging suspicion is becoming established fact. There is growing evidence demonstrating the "apology laws" enacted by most states to protect clinicians after adverse events have little positive effect.

These apologies might even encourage patients to sue, and they can work against a defendant during trial.

Thirty-nine states and the District of Columbia passed apology laws intended to allow physicians and other caregivers to express their remorse over an adverse event or poor outcome without that apology used as evidence of guilt in malpractice litigation. The laws were enacted as the medical community moved away from a previous stance of discouraging apologies to encouraging a more compassionate discourse with patients and family members.

Despite the good intentions of state legislators, the laws were met with some skepticism from the start by the legal community. After years of experience with the laws, many are saying apology laws do not work.

> "THE PATIENT CAN BE INJURED THROUGH JUST BEING UNLUCKY, BUT ONCE YOU GIVE THAT APOLOGY, THE PATIENT CAN CONCLUDE THAT THE DOCTOR THINKS HE SCREWED UP."

Researchers from the Case Western Reserve University Department of Psychiatry in Cleveland and the Department of Psychiatry at Saint Louis (MO) University School of Medicine concluded, "These laws have not yet had their intended effect of reduced malpractice rates, likely because most apology laws protect expressions of regret but do not protect error disclosure. Apology laws therefore do

Financial Disclosure: 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. The relevant financial relationships listed have been mitigated. None of the remaining 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
customerservice@reliasmedia.com
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. California Board of Registered Nursing, Provider CEP#13791.

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

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

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

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

not facilitate the type of communication that would improve physician transparency and overall patient satisfaction."[1]

The two types of apology laws are full and partial. The report explains full apology laws protect statements that are "consistent with the definition of an apology, i.e., an expression of regret and a disclosure of error. States with full apology laws explicitly protect statements of fault." For example, Arizona's apology law protects "any statement, affirmation, gesture, or conduct expressing apology, responsibility, liability, sympathy, commiseration, condolence, compassion, or a general sense of benevolence" from being admitted as evidence.[1]

Most state apology laws do not go that far. Partial apology laws protect "expressions of regret only, without any protection given to error disclosure," the researchers explained. Most apology laws only protect sympathetic statements and offer no protection to explicit expressions of fault.

May Encourage Lawsuits

An unintended effect of apology laws is they might encourage patients to sue after an adverse event, says **Benjamin J. McMichael**, JD, associate professor of law at the University of Alabama School of Law in Tuscaloosa. In a 2019 paper, McMichael explained the underlying assumption of these laws is that an apology will make patients less likely to pursue malpractice claims and more likely to settle claims that are filed.

"However, once a patient has been made aware that the physician has committed a medical error, the patient's incentive to pursue a claim may increase even though the apology itself cannot be introduced as evidence," McMichael and colleagues noted.[2]

Part of the problem is apology laws might encourage clinicians to apologize to a patient without knowing the proper way to do so, McMichael says. Risk managers often train clinicians on how to properly apologize without implying anyone did anything wrong, but those without such training might make statements to the patient causing concern about why the outcome was not as desired.

Apology disclosure programs within hospitals, in which clinicians are coached on how to properly communicate their remorse and regret, have been shown to be effective, McMichael explains. State apology laws seem to make it easier to implement such programs within healthcare organizations because they assure risk managers and other hospital leaders that an apology

EXECUTIVE SUMMARY

State laws protecting clinicians who apologize after an adverse event appear to have little positive effect. They do not reduce malpractice rates.

- The laws are intended to encourage communication with patients without an apology used as evidence of guilt in court.
- Apologizing might alert patients to the possibility of malpractice and lead to lawsuits.
- Most states have some type of apology law.

cannot be de facto evidence of guilt in a malpractice case.

"To the extent that they encourage hospitals to set up these programs, apology laws are useful in that way," McMichael says. "Otherwise, I would say they are useless."

Risk managers should encourage physicians to apologize only if they have been properly trained, McMichael says. If they have not been coached on apologies through a program, the risk manager should advise the physician not to communicate states of regret or remorse following an adverse outcome.

"Your advice to the physician after a bad outcome should be entirely dependent on the training that physician has received and the resources available to him or her through an apology disclosure program," McMichael says. "It should have nothing to do with whether an apology law has been passed in your state."

Even with training and the most carefully worded apology, communication still can prompt a malpractice lawsuit.

"All you're really doing is signaling to the patient that 'you're injured because I screwed up,'" McMichael explains. "The patient can be injured through just being unlucky, but once you give that apology, the patient can conclude that the doctor thinks he screwed up. Even though the apology itself can't be used in court, the patient talks to an attorney and they find information to allege that the doctor was at fault, completely separate from the apology itself."

Apologies Can Be Used Against Physicians

In some cases, plaintiffs' attorneys have used apology laws against clinicians during malpractice trials, says **Roger Harris**, JD, partner with Swift Currie in Atlanta. Georgia's expansive apology law protects most statements conveyed as part of an apology to the patient or family, but Harris has seen attorneys use it to prevent clinicians from expressing regret or remorse when testifying as part of a malpractice trial.

The plaintiff's attorney can successfully argue the apology law means any type of apology or expression of compassion is inadmissible and not permitted during testimony. That was not the intent of the legislature when it passed the apology law, but because of plaintiff's attorneys using it against physicians, Harris calls the Georgia apology law "the anti-human being statute."

"They assert that the stature prevents what any reasonable human being would want to do at the point they take the stand in the trial — which is very often the first time they're encountering these family members again — and that is to take the stand and say, 'I'm sorry this happened,' or 'I'm sorry this was the outcome, but I don't believe I deviated from the standard of care,'" Harris explains. "As opposed to being a shield, it became a sword to prevent the jury from being able to see and appreciate that these healthcare providers were, in fact, real human beings with real human feelings and real human emotions."

Clinicians struggle to testify without stating any concern for the patient and family members or saying they regret how the case turned out, Harris says. The jury might view the doctor as having no feelings or emotions about the case, which is usually far from the truth.

The law has only negatively affected malpractice cases in Georgia, with none of the intended effect of encouraging honest communication with patients and families, in Harris' estimation.

"In those moments after a poor outcome, people are going to say what they need to say to the patient and family members in terms of being sorry and regretful about the outcome," Harris says. "Doctors and nurses and other providers are not thinking about the statute when they are dealing with a distressed family. This statute is hardly even talked about anymore, except when plaintiffs' lawyers file motions to

preclude statements at the time of trial."

Several states, including Arkansas, have not passed apology laws, notes **Jason B. Hendren**, JD, partner with Hall Booth Smith in Rogers, AR. In those states, an apology still puts a clinician at risk of the statement being used as evidence of wrongdoing.

Hendren defended a physician in a case in which the main liability argument was that his client used the phrase "this is the worst day of my life" when informing a family of an unexpected, but non-negligent, surgical complication.

"He was trying to be empathetic, but it backfired. Although the jury returned a unanimous defense verdict, it was extremely frustrating for the provider to know that his own words likely brought about the lawsuit and were used against him, over and over, during the trial," he says. "The experience made him wary of his communications with patients and their families. Moreover, and most regrettably, he lost much of the enjoyment of practicing medicine."

Risk managers should know the laws in their respective jurisdictions and encourage a collaborative approach with providers to determine what language is used in communicating with patients and their families about adverse events or outcomes.

"I have no doubt that my client would have benefited from being advised beforehand that a comment like 'this is the worst day of my life,' however well-meaning, would not be optimal in explaining what he knew to be an unexpected, but non-negligent, surgical complication," Harris says.

Partial apology laws, the most common type, require the clinician to understand what is and is not protected. For example, if a provider in a partial apology law state admits "operating on the wrong knee," and she is "sorry" about it, the only admissible portion of the statement would be the part about operating on the wrong knee, since that is a medical fact, Harris explains. The expression of sorrow would not be admissible because it is not a medical fact and cannot be admitted into evidence to prove fault.

PARTIAL APOLOGY LAWS MIGHT LEAVE CLINICIANS WITH SEMANTIC CHALLENGES THAT CAN MAKE THEM SOUND INSINCERE, OR EVEN SUSPICIOUS.

Partial apology laws might leave clinicians with semantic challenges that can make them sound insincere, or even suspicious, as they attempt to guide their comments along the narrow path of protected words.

"There are those who argue that jurisdictions with no apology laws are best because the lack of such laws removes the issue of admissibility from consideration and encourages language that is more explanatory rather than fault or sympathy-based," Harris says.

Regardless of which state laws apply, Harris says risk managers should encourage providers to communicate with patients and their families with empathy and honesty during all stages of care and treatment. Building trust before an adverse event or outcome occurs will be important in how subsequent discussions are received.

Patients and their families often are more concerned about knowing what happened, how they will take care of the patient going forward, and how similar situations will be addressed or prevented in the future, rather than knowing who is to blame for what happened.

"Unfortunately, apologies are rare in our society, and that sometimes makes them sound suspicious — even when they are sincere and well-intended. Awareness of this cultural fact and how it affects open and honest communications with patients and their families is imperative in professional healthcare relationships," Harris says. "Difficult conversations are necessary from time to time, but providers need to recognize that it is not just how you say things, but what you say." ■

REFERENCES

1. Ross NE, Newman WJ. The role of apology laws in medical malpractice. *J Am Acad Psychiatry Law* 2021;49:406-414.
2. McMichael BJ, Van Horn RL, Viscusi WK. "Sorry" is never enough: How state apology laws fail to reduce medical malpractice liability risk. *Stanford Law Rev* 2019;71:341-409.

SOURCES

- **Roger Harris**, JD, Partner, Swift Currie, Atlanta. Phone: (404) 888-6175. Email: roger.harris@swiftcurrie.com.
- **Jason B. Hendren**, JD, Partner, Hall Booth Smith, Rogers, AR. Phone: (479) 391-6202. Email: jhendren@hallboothsmith.com.
- **Benjamin J. McMichael**, JD, Associate Professor of Law, The University of Alabama School of Law, Tuscaloosa. Email: bmcmichael@law.ua.edu.

Prepare Now for Critical Device Security Incidents

Hospitals and health systems are increasingly dependent on sophisticated medical devices for patient care and maintaining safety, but not all are ready to respond effectively when hackers access those devices. Risk managers should ensure an effective response plan is in place that is well practiced and ready to deploy at a moment's notice.

The Cloud Security Alliance (CSA) in Seattle recently released its *Medical Device Incident Response Playbook* to help healthcare organizations respond when hackers compromise devices. The group said the guidance was inspired by growing medical device security concerns since the 2017 WannaCry ransomware incident, which successfully encrypted radiology equipment drives at hospitals.

"While serious confidentiality and integrity issues are often associated with leakage of medical device data, the highest risk when dealing with systems being used for clinical care concerns is keeping those systems available for patient care use," the authors stated.[1]

The biggest risk is medical devices will be taken offline or compromised in ways that threaten patient safety. A malpractice lawsuit against an Alabama hospital alleges a newborn child died because of a ransomware attack that affected specific medical devices and the hospital's computer systems. *(For more information, see the December 2021 issue of* Healthcare Risk Management *at: https://bit.ly/3opTSDT.)*

Cyberattacks can affect a wide range of computer operations, but the CSA report focuses on how to respond when individual medical devices or a type of device is affected.

Playbook Guides Emergency Response

The CSA playbook was co-authored by **Brian Russell**, chief technology officer of TrustThink, a cybersecurity company in San Diego, and **Christopher Frenz**, CISSP, HCISPP, CISM, CISA, FIP, CIPP/US, CIPM, CIPT, CCSK, assistant vice president of IT security at Mount Sinai South Nassau in Oceanside, NY.

The playbook emphasizes the risk to patient care from a cyberattack, Frenz notes. Cybersecurity efforts often focus on the many other types of cyberattack damage, including financial, operational, and privacy threats, but the direct risk to patients can be underestimated.

"That's one of the things that is largely missing from the conversation today. There needs to be a patient safety focus with cybersecurity decision-making, both on the protection side and also on the incident response side," Frenz says.

The FDA has worked to ensure better security for the next generation of medical devices. But some legacy systems still function perfectly well in a clinical sense, and remain in use.

"There are a lot of very vulnerable medical devices in hospitals, and there will be for some time," Frenz says.

Medical devices increasingly are interconnected with systems outside the hospital walls, making them targets for hackers, Russell says. Compromising patient safety might not necessarily be the hacker's intent, but the medical device at the bedside can be a convenient way to gain access to other hospital systems.

"As these devices become more sophisticated and interconnected, there are a lot of opportunities for the bad guys to use them as entry points into the hospital enterprise network as well," Russell says. "You have to be vigilant that you're only allowing secure devices on your network."

Devices Can Be Entry Point

Medical devices sometimes are a weak link in a hospital's overall cybersecurity program, says **Rich Temple**, vice president and chief information officer of Deborah Heart and Lung Center in Brown Mills, NJ. For instance, many devices are shipped with a default password that some hospitals never change.

"If a bad guy were to get their hands on this default password, they could do a lot of damage," Temple says. "Another big problem with medical devices is that I can [perform] a vulnerability scan on my network without adversely affecting

EXECUTIVE SUMMARY

Hackers can compromise medical devices in ways that can threaten patient safety. Healthcare organizations should prepare to respond to medical device safety incidents and minimize the risk to patients.

- The number of devices used for critical patient care is increasing rapidly.
- Hospitals should create a response plan that can be activated immediately.
- Practice the response plan the same as with other disaster plans.

operations, but I have to be much more prescriptive and careful about [performing] scans on my medical devices because that device might be attached to someone and providing life-affirming care. A scan could knock that device offline."

Hospitals should train staff and physicians to raise an alarm if they suspect a medical device is not performing normally, Temple says.

Most healthcare organizations probably are not as prepared to deter and respond to a medical device incident as they are with other types of security breaches.

"It's trickier and involves a lot more moving parts," Temple says. "You have to accept that this is an issue we need to address, working very closely with biomedical engineering, and sometimes the IT department, to ensure we have processes in place to detect default passwords and avoid breaches."

The hospital also should create a detailed response plan that includes steps for allowing the device vendor to access the equipment, which Temple says must be limited and monitored by hospital representatives.

"Fortunately, attacks on medical devices have not been as frequent as the more conventional network attacks, but that could change quickly. This could be the next big vector for attacks," Temple warns. "I think we have a chance to get ahead of it, but not much time."

More Dependence on Devices

Action is needed because healthcare providers are increasingly dependent on these devices to provide safe and effective patient care, notes **Philip J. Bezanson**, JD, managing partner with Bracewell in Seattle. Currently, there are about 12 medical devices per hospital bed, but industry experts expect that number to triple in the next five to 10 years.

"That is a ton of equipment, and each item needs to have its own mini-playbook for responding to a compromise. You have to know if the problem is with just this one device, or is every one just like it at risk," Bezanson says. "What is the risk? Is it just a data collection risk, or is it a functionality risk where there can be real harm to a patient?"

MOST HEALTHCARE ORGANIZATIONS PROBABLY ARE NOT AS PREPARED TO DETER AND RESPOND TO A MEDICAL DEVICE INCIDENT AS THEY ARE WITH OTHER TYPES OF SECURITY BREACHES.

The risk might be greatest for hospitals that did not employ the internal resources to address previous cybersecurity threats and had to outsource the efforts to protect networks from data breaches, Bezanson says. Without a strong internal team with experience in protecting the hospital's network, they might face a bigger challenge in taking a proactive approach to medical device security.

Risk managers should view a medical device security response plan as similar to other disaster response plans. When a natural disaster strikes the hospital, a plan is activated immediately and various people will know their roles. The same sort of response should trigger when a medical device is compromised.

"We've reached the stage where things move so quickly that you may have to make decisions very quickly about pulling devices offline and taking other steps," Bezanson says. "You won't have the time to pull a binder off the shelf and see what you're supposed to do. You have to have a team that already knows."

Must Practice Response Plan

Another key aspect of a cybersecurity strategy is practicing incident response procedures, says **Brian Wrozek**, chief information security officer at Optiv Security in Denver.

One cannot stop every attack, so be ready to respond and minimize the damage, Wrozek says. One option is seeking help from third-party providers who specialize in incident response. Add clauses to contracts that require vendors and suppliers to participate in incident response drills and be ready to respond in an emergency. *(See the related story in this issue for more information on how to include vendors.)*

The response plan should incorporate law enforcement. Wrozek advises building those connections now. Do not wait until the attacker has struck.

"Don't forget to follow any requirements from your insurance provider and related industry regulations. These exercises should include all aspects, from technology concerns to communications," Wrozek says. "Be prepared to deal with social media and misinformation. Have a plan for

communicating not only with patients and the public at large, but also employees and partners. Transparency is key to maintaining public confidence and trust."

Can Migrate from Other Devices to Medical

One important consideration is cyberattacks can originate from any connected devices, not just medical gadgets, says **Greg Murphy**, chief executive officer of Ordr, a cybersecurity company in Santa Clara, CA. For example, if connected devices, like an HVAC control system, elevator control systems, or building management system, are compromised, an attacker can move laterally to a connected medical device.

When a cybersecurity incident happens, Murphy suggests thinking of the response in four parts:

- Understand what device has been compromised;
- Pinpoint its network and physical location;
- Determine if you can act on the device;
- Determine exactly what response is possible.

Understanding which device has been compromised is fundamental, Murphy says. It is crucial for an organization to maintain a continually updated, referenceable, real-time connected device inventory database. This database should classify devices based on their risks so the security team can individually prioritize alerts and responses.

Next, knowing the physical and network location could be critical for a technician to locate the device to take it off the network or determine what compensating control is possible based on its network connectivity.

These details are fundamental to determining whether action can be taken and exactly what type of action can be performed on the compromised device, Murphy says. For example, the clinical team might not be able to take a compromised MRI machine offline because of the negative effect to patient care. The proper response may be to quarantine the device.

"This is where mapping and baselining the behavior and communications patterns of a device using machine learning can accelerate the creation of the right segmentation policies to isolate the device and prevent lateral movement," Murphy says.

Access to All Devices Possible

Once cybercriminals gain access to a healthcare network, they often can access all devices connected to it, notes **Troy Ament**, field chief information security officer for healthcare at Fortinet in Sunnyvale, CA. Compromising those devices and threatening patient safety can be a way to pressure hospitals to pay ransomware.

Organizations should ensure advanced security (e.g., anti-exploit and endpoint detection and response) is installed in all endpoint devices, Ament says. These tools can discover malware on an endpoint device before it migrates to the network and shares that information downstream.

"We also can't ignore the importance of teaching good cyber hygiene. Users must be part of the solution, which means all employees must receive training from the get-go. It must be a continuous learning process, and employees need to learn how to spot and report suspicious cyberactivity," Ament says. "This can be challenging in a medical environment, since priority one needs to remain patient care."

The key to a successful security program is its alignment with business mission and objectives, says **William Mendez**, managing director of operations with CyZen in New York City. Unfortunately, many security professionals create a myopic view of security, and only consider the controls and the obstacles.

"They fail to consider the impact that controls have on business operations, and do not seek that balance where security is applied, but the organization can still function as a business to meet its goals," Mendez says. "After all, a business that cannot meet its goals will not be in business for long. Or, in the case of medical devices, failure to achieve this balance can be a matter of life and death."

Medical device security brings this dilemma to the forefront, Mendez says. These devices are built for a specific purpose, and security usually is not at the top of its list of features. They usually consist of embedded operating systems that usually are "stripped down" versions and often cannot support traditional security protocols or mechanisms such as antivirus software, says **Michael Schenck**, senior cyber security consultant with CyZen.

Healthcare organizations should run a risk evaluation on new or upgraded software or hardware before introducing it to patient care, Schenck says.

A common security measure is to ensure software and hardware are fully patched, but Mendez explains because their internal operating systems have limited capacity, standard patching of medical devices can cause more harm, destabilizing the system and potentially affecting its operation.

"As a result, we have to rely on the vendor to provide patches, which can take longer to be released than a regular patch," Mendez says. "This increases the window of opportunity for a threat actor to exploit an existing vulnerability." ■

REFERENCE

1. Cloud Security Alliance. *CSA Medical Device Incident Response Playbook.* Nov. 8, 2021. https://bit.ly/31fu3O5

SOURCES

- **Troy Ament**, Field Chief Information Security Officer, Healthcare, Fortinet, Sunnyvale, CA. Phone: (408) 235-7700.
- **Philip J. Bezanson**, JD, Managing Partner, Bracewell, Seattle. Phone: (206) 204-6206. Email: philip.bezanson@bracewell.com.
- **Christopher Frenz**, CISSP, HCISPP, CISM, CISA, FIP, CIPP/US, CIPM, CIPT, CCSK, Assistant Vice President, IT Security, Mount Sinai South Nassau, Oceanside, NY. Phone: (516) 632-3000.
- **William Mendez**, Managing Director, Operations, CyZen, New York City. Phone: (212) 842-7005.
- **Greg Murphy**, Chief Executive Officer, Ordr, Santa Clara, CA. Phone: (833) 673-7999.
- **Brian Russell**, Chief Technology Officer, TrustThink, San Diego. Email: russell_brian@trustthink.net.
- **Michael Schenck**, Senior Cyber Security Consultant, CyZen, New York City. Phone: (212) 842-7005.
- **Rich Temple**, Vice President, Chief Information Officer, Deborah Heart and Lung Center, Brown Mills, NJ. Phone: (609) 893-6611.
- **Brian Wrozek**, Chief Information Security Officer, Optiv Security, Denver. Phone: (800) 574-0896.

Contact Manufacturer When Medical Device Is Compromised

The response plan for a compromised medical device should include contacting the device manufacturer, advises **Richard Sheinis**, JD, partner with Hall Booth Smith in Charlotte, NC.

Check if any security updates or patches were missed, and know what type of patient data are collected, stored, or transmitted by each device, he says. Review any logs maintained by the device to determine if it was accessed by an unknown IP address.

Follow the connectivity of the device to other components of the computer network to find out if other components were accessed through the device. Take the device offline and disconnect from the patient if safe to do so.

Maintain the device for a subsequent forensic review. Check other devices to determine if they have been compromised as well.

"Consider taking all such devices offline until they can be assessed for security vulnerabilities. This might not be possible for all devices, such as implanted devices," Sheinis says. "Have an inventory of medical devices and know the clinical impacts of security incidents that affect the different devices. Have substitute or backup devices available to replace the compromised device and any other devices taken offline."

Before acting, always know the effect on patient safety for each of these actions.

The security of medical devices should be addressed from the time the medical provider contracts to purchase the device, Sheinis says. Obtain information from the manufacturer regarding the security of the device, such as the Manufacturer Disclosure Statement for Medical Device Security (MDS^2). The contract should address which party is responsible for maintaining and updating the device's security.

"If a security patch is issued, which party is responsible for applying the patch in a timely manner? Does the manufacturer have cybersecurity practices in place to prevent unauthorized access to the device?" Sheinis asks. "Does the manufacturer update the security of the device, including software changes?"

A medical device is an endpoint of the computer system, similar to a laptop computer as an endpoint, Sheinis notes. Endpoint monitoring should include medical devices (when possible), and medical devices should be included when the medical provider conducts vulnerability testing. Cybersecurity vulnerabilities have been found in wireless telemetry, insulin pumps, imaging devices, implantable cardiac devices, and infusion systems, he says. ■

SOURCE

- **Richard Sheinis**, JD, Partner, Hall Booth Smith, Charlotte, NC. Phone: (980) 859-0381. Email: rsheinis@hallboothsmith.com.

Cyberattacks Increasing Since Pandemic Began

Since the beginning of the pandemic, the healthcare industry has seen a significant rise in cyberattacks, says **Heather Paunet**, senior vice president of products at Untangle, a cybersecurity firm in San Jose, CA.

The combination of the pandemic's effects — crowded facilities, expanded telehealth usage, exhausted workers — with more reliance on medical devices has left the industry vulnerable to cybercriminals.

"While medical devices, which are connected to the internet and hospital networks, enable physicians to easily access and share critical medical information and have greatly improved the performance and effectiveness of medical centers, they make healthcare systems prime targets for hackers," Paunet says. "Unfortunately, due to the critical patient data they hold, supplemented with key personal identifiers, medical organizations have become common targets for attacks."

Healthcare IT security teams should update, monitor, and test their networks and connected systems daily, Paunet says. They also should develop and implement a risk assessment plan to understand threats to the network and create mitigation or remediation plans.

Network administrators must be prepared to quickly access backups and restore functionality, which requires knowledge of what data were backed up, when it was backed up, where the backups are stored, and what is needed to restore them. Paunet says a cybersecurity incident response plan should include these steps:

- **Detection and analysis:** Implement warning systems that alert when a breach or attempted breach has occurred.
- **Immediate response:** Develop an immediate and robust response to close the breach and prevent further infiltration.
- **Containment:** Contain the breach to further prevent data loss and to block sharing of data.
- **Eradication:** Close and eradicate the vulnerability.
- **Recovery:** Ensure business continuity or resumption of operations and set actions in motion to remediate reputational damage.
- **Reporting:** Examine the circumstances surrounding the breach to learn from it and review the response to find ways to improve the plan.

In addition, Paunet advises healthcare organizations to implement these steps to prevent cyberattacks:

- **Deploy the right tools to monitor devices and activity.** All desktops, laptops, mobile devices, and medical devices connected to the network should be monitored, and complete network activity reports maintained. It also is important to keep all software and protections up to date. Never skip or delay an update.
- **Isolate the effect of a potential attack.** Creating separate networks for different purposes can ensure any attack is isolated, hopefully keeping damage to a minimum. For example, putting all internet-connected devices on a separate network away from servers used for day-to-day data exchanges will ensure those servers will not be affected in the event of a breach.
- **Back up data regularly.** Back up data daily and continuously scan to ensure backups are free of malware. Performing multiple backups also is recommended, as this provides extra insurance if there are problems with the previous day's backup. Go back one day to ensure a clean restore.
- **Enforce password policies and deploy multifactor authentication.** With employees in constant contact with sensitive personal information, password security is paramount. It is important to use strong passwords — combinations of characters, symbols, and numbers that cannot easily be guessed — and change them regularly.
- **Use two-factor authentication.** This can add an additional layer of defense to any login or credentialed-access portal. ■

SOURCE

- Heather Paunet, Senior Vice President of Products, Untangle, San Jose, CA. Phone: (866) 233-2296.

Recruitment Agreements Run Risk of Stark Law Violations

Hospitals may enter into recruitment agreements to bring needed physicians into the community. However, serious legal issues can arise related to the Stark Law, which prohibits making referrals involving a compensation arrangement or investment interests.

A physician who feels misled by an agreement could blow the whistle on potential Stark violations. The issue often comes down to proving the recruitment agreement was necessary because the community was in dire need of the physician services, says **Ericka L. Adler**, JD, shareholder with Roetzel & Andress in Chicago. Simply saying there was a need is not enough; the hospital must prove the need was researched and documented.

Recruitment Exception

The Stark Law allows a recruitment exception for hospitals to provide money to doctors and physician groups even though they are in a position to refer patients to the hospital, but only when certain conditions are met, Adler says. Those conditions include proving a physician shortage in the area, and the physician is coming from far enough away that they do not already see patients in the area.

Hospitals may recruit specialty physicians for care not available in the community, and the agreements can involve hundreds of thousands of dollars. Adler represents physicians and has been involved with a recruiting agreement concerning more than $1 million. Typically, the agreements require the physician to practice in the community for a specified period. In the beginning, the hospital provides monetary support until the doctor's practice is established.

Physicians May Challenge Agreement

The recruitment agreement provides a salary guarantee for the physician and reimbursement of expenses, usually to a physician group.

"You have a lot of money pouring from the hospital to group and the physician. It's nice for the physician when the money is flowing, but then the physician is required to stay in the community to earn forgiveness for that compensation, usually between two and four years after they've gotten the money," Adler explains. "Suddenly, there's not enough work to do, and the steady income from the hospital isn't there anymore."

At that point, the physicians might question the hospital's original claim of a real need for their services. If the physicians want to leave the community, they must pay back the money received from the hospital, Adler says. The physicians often are young and naïve, and they feel trapped by what they see as disingenuous claims by the hospital.

If the physicians challenge the recruitment agreement, the hospital could be accused of violating Stark, Adler explains. She has been involved in settlement discussions with hospitals in which they backed down from enforcing the recruitment agreement once her physician client raised the possibility of reporting a Stark violation.

"The physicians are not in a position to know the truth of whether there is a real need in the community, so when the hospital says there is and they offer all this money to come and practice there, the doctors sign the agreement," Adler says. "When push comes to shove, we have to tell the hospital we believe there was no need and this was a violation of Stark recruitment exception, and if they insist on suing the physician, we will make that known. They usually back down because they know they are at real risk there."

If federal authorities questioned the claim of community need, the hospital would have to prove that it conducted thorough research and show documentation of the need for particular types of physicians, Adler says. A general sense of need would be insufficient.

EXECUTIVE SUMMARY

Hospitals may recruit and compensate physicians under an exception to the Stark Law. Community need is a key component.

- Hospitals must prove certain physicians are needed in the community.
- Reimbursement of expenses also can be abused.
- Stark Law violations may be alleged if physicians want out of a recruitment agreement.

Reimbursement for expenses also can be problematic. The Stark exception allows reimbursement only for incremental expenses, meaning whatever costs the physician group incurred by adding this physician, such as building office space.

"What we often see is that the hospital is paying for a portion of the overall overhead of the group, and that is a violation of the recruitment exception. We have pointed this out many times to hospitals, and they may care or not care because there often is an overly friendly relationship between the hospital and the group, with an endless rotation of physicians, and the group being paid over and over again," Adler says. "The physician can be at a disadvantage if they don't look at these agreements carefully, but the hospital can be at risk of Stark violations if a dispute results in any of this coming to light." ■

SOURCE

- **Ericka L. Adler**, JD, Shareholder, Roetzel & Andress, Chicago. Phone: (312) 582-1602. Email: eadler@ralaw.com.

Latest Leapfrog Safety Grades Include Post-Op Sepsis

The most recent grades from The Leapfrog Group represent the largest set of hospitals ever evaluated, with grades assigned to 2,901 facilities. More than 30 evidence-based measures of patient safety were assessed, including postoperative sepsis, blood leakage, and kidney injury for the first time.

New Measures Included

The report includes 200 more hospitals than were previously graded, says **Erica Mobley**, director of operations with The Leapfrog Group. Methodology updates enabled them to include the CMS measure PSI 90, a composite measure of several patient safety errors.

"By including PSI 90, we were able to capture safety errors that were not included in the safety grade, but it also allows us to measure hospitals that might have slightly lower volume and previously were not able to report on some of the other measures," Mobley says. "It's great to be able to include more hospitals. We update our methodology so that we are always incorporating the most current evidence-based measures of safety. This was an exciting measure to include this time around."

There was improvement in two process measures related to medication safety: *Clostridioides difficile* infections and deaths after surgical complications. But there was decline in performance on measures related to central line infections and MRSA, Mobley says.

"There is evidence that some of the patient safety gains we have made in the past may have slipped back during COVID. The most recent report includes some information from 2020, but the majority of the data are from 2019, so I wouldn't say we have seen the full impact of the COVID data yet," she explains. "Hospitals really need to go back and put their focus on these core tenets of infection prevention, with things like checklists and more robust handwashing policies, to get back to the basics that they had been doing so well on."

These are some highlights from the fall 2021 Leapfrog Hospital Safety Grade report:

- Thirty-two percent of hospitals received an A, 26% received a B, 35% received a C, 7% received a D, and less than 1% received an F.
- The five states with the highest percentages of A hospitals are Virginia, North Carolina, Idaho, Massachusetts, and Colorado.
- There were no "A" hospitals in Delaware, Washington, DC, or North Dakota.

The report is available online at: https://bit.ly/3ou3gpL. ■

SOURCE

- **Erica Mobley**, Director of Operations, The Leapfrog Group, Washington, DC. Phone: (202) 292-6813.

COMING IN FUTURE MONTHS

- Fraud disclosure protocol
- A closer look at vaccination policies
- Factors affecting premium rates
- Addressing workplace violence

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 100%; you will be allowed to answer the questions as many times as needed to achieve a score of 100%.

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

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

CME/CE QUESTIONS

1. **How many states enacted apology laws intended to protect clinicians who express regret or remorse after an adverse outcome?**

   a. 12 states, but not the District of Columbia
   b. 24 states and the District of Columbia
   c. 39 states and the District of Columbia
   d. 50 states, but not the District of Columbia

2. **What is one way recruitment agreements can run afoul of the exception allowed under the Stark Law, according to says Ericka L. Adler, JD?**

   a. The hospital cannot sufficiently document the community needed the services of the physician compensated by the agreement.
   b. The hospital terminates the agreement before the specified time.
   c. The hospital provides greater compensation than allowed by Stark.
   d. The hospital recruits more than one physician at a time.

3. **What is one reason medical devices can be a weak link in a hospital's overall cybersecurity program?**

   a. Many devices are shipped with a default password that some hospitals never change.
   b. Many device passwords cannot be changed.
   c. Many devices are not password protected.
   d. Many device passwords are openly posted on the machine.

4. **Which is true of apology laws, according to Benjamin J. McMichael, JD?**

   a. Both state apology laws and hospital disclosure programs are effective.
   b. State apology laws are effective, but hospital disclosure programs are not.
   c. Hospital disclosure programs are effective, but state apology laws are not.
   d. Neither state apology laws nor hospital disclosure programs are effective.

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

Failure to Screen for Cancer, Hepatitis C Leads to $2.7 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: An patient was undergoing regular prostate-specific antigen (PSA) screenings given his particular background and medical history. Despite awareness of the patient's risk factors, a physician failed to order sufficient screenings. Eventually, the patient was diagnosed with and died of prostate cancer exacerbated by hepatitis C. His family sued, alleging his death was caused by a physician's failure to properly screen for cancer and hepatitis C. The jury found the physician negligent and awarded the plaintiffs approximately $2.7 million in damages.

Background: A patient elected to undergo regular PSA screenings because of his age and family history of prostate cancer. His physician was aware of these risk factors, but did not order sufficient PSA screenings to diagnose the patient's prostate cancer at an early stage.

In 2012, the patient's PSA was 1.0 ng/mL. In 2014, the patient's PSA measured 1.2 ng/mL. A year later, the patient's PSA level had tripled to 3.0 ng/mL. The physician failed to order additional tests to detect prostate cancer. Finally, in 2017, the physician ordered another PSA test, which measured more than 250 ng/mL. A prostate biopsy found cancer a few weeks later. Due to the progression of the cancer, the patient passed away in 2018.

The patient also was at high risk for hepatitis C due to his age, history of blood transfusions, and abnormal liver function tests. However, the physician did not order screenings for hepatitis C. At some point, the patient contracted hepatitis C. It continued unchecked until it caused cirrhosis and liver cancer, which contributed to the patient's death.

The patient's surviving family filed a medical malpractice action, arguing the physician's failure to screen was negligent due to the patient's risk factors, including a family history of prostate cancer. Furthermore, he was at risk for hepatitis C because of his age, history of blood transfusions, and abnormal liver function tests. However, the physician ordered infrequent PSA screenings that, if properly ordered, would have detected the patient's cancer earlier.

> THE PHYSICIAN ORDERED INFREQUENT PSA SCREENING THAT, IF PROPERLY ORDERED, WOULD HAVE DETECTED THE PATIENT'S CANCER AT AN EARLIER STAGE.

The patient's family alleged these failures constated medical malpractice, as a reasonable physician in the same or similar circumstances would have ordered additional testing and monitored the patient closer. The defendant physician denied liability, arguing the patient's own actions contributed to his injuries and death because he failed to follow the physician's order and obtain timely lab work. During jury selection, eight medical professionals — ranging from nurses to hospital administrators — were selected.

After four hours of deliberations, the jury found the physician's failure to screen the patient and failure to act on the patient's abnormal PSA values enabled his cancer to advance, which led to his death. The jury also found

these failures fell below the applicable standard of care; thus, the physician was negligent.

The jury awarded $3 million to the patient's surviving family. Half was allocated to the patient's pain and suffering caused by undiagnosed prostate cancer, and half was allocated to pain and suffering because of the undiagnosed hepatitis C. The jury partly agreed with the physician's defense and found the patient was 20% at fault for the undiagnosed hepatitis C, since the patient failed to obtain lab work on one occasion. The verdict was reduced by $300,000 to correspond with the patient's fault, bringing the award to $2.7 million. The family's attorney credited the quick verdict to the eight medical professionals on the jury because they could easily recognize the lapse in the standard of care.

What this means to you: This case illustrates the importance of risk factors in setting the standard of care for medical screenings and testing. Many patients will not require frequent screening for prostate cancer and hepatitis C. However, for certain patients, such as the one in this case, risk factors require a physician to take a different course of conduct. Because of this patient's litany of risk factors, the physician should have ordered additional or more frequent screening and testing.

Discussing a patient's history and background, including the patient's family medical history, is important for a physician to determine the applicable standard of care. It is important for physicians and care providers to listen to patients, not only about their current symptoms, but also to listen to the patient's history. Every patient is different. The individual is in the best position to relay the underlying data to enable a physician's diagnosis. Physicians and care providers should be cautious about making assumptions or disregarding data provided by patients. A physician who fails to inquire about relevant current or historical information, or who fails to act after receiving such information, may be committing malpractice.

In this case, the physician knew about the patient's significant risk factors, yet failed to take appropriate action. This patient was a primary candidate for more screenings for good reason — and the unfortunate reality is the patient did eventually develop prostate cancer at a young age. While that inevitability would not have been prevented, if the physician would have adhered to the applicable standard of care, the patient's cancer could have been detected far earlier and have been treated more aggressively and timely.

It is unclear why the physician failed to order the timely screening, or why the patient contributed to these screening failures by not appearing for ordered testing. One potential explanation is that with the ongoing pandemic, rates of preventive care, screening, and non-emergency care have declined. Many providers have experienced this firsthand, whereby patients put off care that otherwise would have been a matter of course. Adapting to this current reality may be challenging, and physicians and care providers can only do so much to encourage patients to adhere to orders or to seek testing when risk factors indicate such screenings are warranted.

While it is the physician who provides the care, it is incumbent on the patient to seek out the physician — and to follow through. Physicians and providers cannot force patients to seek or receive treatment or testing, even when such testing could be life-saving. In the context of a medical malpractice action, it might be possible for a care provider defendant to demonstrate the patient's own actions caused the injury. There are various legal terms and differences among jurisdictions about exactly how these doctrines apply; generally, liability correlates with fault. If the patient is at fault for his or her own injury, then the patient could be precluded from recovering any damages, or their damages may be reduced.

In this particular jurisdiction, the jury attributed 20% of the fault to the patient and reduced the monetary damages accordingly. Physicians and care providers can take solace when they have advised a patient on a certain course of treatment or testing, and the patient then fails to adhere to the advice. It might be a sensitive topic to broach in a malpractice action, particularly where the patient has actually suffered grievous injury or death, because it could be perceived as attacking the victim. But patients are not always blameless in their own injuries. When that is the case, it is absolutely appropriate for physicians and care providers to cautiously demonstrate the patient might have contributed to his or her own injury.

Yet another lesson from this case is the importance of jury selection. It is surprising that eight medical professionals served on the jury, simply because juries are selected from the voting population as a whole. The odds of including so many within the medical field for a medical malpractice action is rare. Jury selection is a complicated process, and it often is difficult to speculate about the outcome based solely on the jury selection. In this case, the jury's deliberation could indicate the jury's inherent medical knowledge facilitated the swift resolution with a four-hour

deliberation for this multimillion-dollar verdict. The laypersons on the jury may have simply deferred to the medical professionals, who quickly determined they would have acted more cautiously or differently given a similar patient. It is far more common for a jury to be more balanced and to possess less inherent knowledge, which may facilitate a physician or care provider's presentation of expert testimony critical for defense. ■

REFERENCE

- Decided Oct. 22, 2021, in the Court of Common Pleas, Philadelphia County, Pennsylvania, Case Number 1804-04705.

Injury from Botched Hip Surgery 'Speaks for Itself' in Negligence Case

News: A patient underwent hip replacement surgery, after which he exhibited femoral nerve palsy. Tests confirmed permanent nerve damage. The patient filed a malpractice action, alleging the permanent nerve damage must have been caused by the physician's negligence.

A trial court initially dismissed the malpractice action because the patient could not specifically identify the negligent acts. However, the patient appealed, and the appellate court reversed the dismissal. It agreed that absent negligence, permanent nerve damage does not occur. The patient was permitted to bring his action.

Background: In October 2016, an adult male underwent hip replacement surgery. After the surgery, the patient exhibited femoral nerve palsy. Testing confirmed nerve damage in his quadriceps, including severe left femoral neuropathy specific to the branches to the vastus lateralis and rectus femoris muscles. A lesion appeared complete with no evidence of voluntary motor unit potential activation.

In September 2018, the patient filed a medical malpractice suit. The patient did not name any specific wrongdoing by the surgical team, but still claimed the fact he suffered permanent nerve damage means medical malpractice must have occurred. The discovery process did not reveal any provider mistakes. The defendant physician and surgical team all denied liability and claimed they performed the surgery in accordance with the applicable standards of care.

The defendants filed a motion to dismiss the case based on the patient's inability to demonstrate any breach of the standard of care. As the plaintiff, a patient is required to provide evidence concerning each element to prove malpractice, including the provider's actions breached the standard of care. The patient was under anesthesia during the procedure, and no written evidence or testimony revealed any error. Since the patient could not demonstrate an action that fell below the standard of care, the court dismissed the case.

The patient appealed the dismissal, and the appellate court reversed. The primary basis for the appeal was a legal doctrine, known as "res ipsa loquitur," that the patient raised, but the trial court rejected. The basis of this doctrine is that when an injury cannot happen without negligence, there must be negligence if an injury occurred. Thus, even if a patient — or anyone else — did not observe the act that caused a harm, the act still must have happened if the patient suffered the harm. Under this doctrine, a patient is relieved of the need to connect the specific act that caused the harm as long as the patient puts forth sufficient evidence to demonstrate such an injury.

The appellate court agreed with the patient. In this case, the patient's expert testified permanent nerve damage does not occur outside negligence. Specifically, the patient's expert testified he had performed hundreds of hip replacement surgeries and had never encountered injuries like the patient sustained. In his opinion, nerve injuries could occur during non-negligent hip replacement surgery, but they would not be permanent. Moreover, the expert had never seen nor read about the types of injuries the patient suffered occurring, absent negligence. This testimony was enough to reverse the dismissal of the patient's case and permit the case to move forward.

The court analogized the case to one where a surgical sponge is left inside a patient. In that case, it is obvious someone was negligent, even if the surgical team and records report that no errors occurred. Here, the patient's expert established the nerve damage was like the surgical sponge: Neither a forgotten surgical sponge nor permanent nerve damage happen without negligence. In both cases, the injury speaks for itself, and is sufficient to support a jury trial on the issue of negligence.

The court also spoke on the issue of the applicable standard of care

when res ipsa loquitor is invoked. Under this doctrine, the patient did not need to establish the applicable standard of care. The injury established the defendants had a duty to exercise ordinary care and not injure the patient by violating that standard.

The also court ruled on an additional matter. A surgical technician argued she should be dismissed from the case because she acted entirely under the direction of the surgeon; therefore, any error was his for which she could not be liable. The court disagreed, stating if the surgical technician was dismissed, then the surgeon could argue her negligence caused the injury, not the surgeon's. Therefore, both the surgical technician and the surgeon remained in the case, and it is up to a jury to determine whether liability exists and to apportion it to either, or both, defendants.

What this means to you: This case presents an interesting intersection between the facts and the law. Does the legal system compensate a patient who indisputably suffered a significant, permanent injury when an investigation cannot reveal how the injury occurred? In this case, the patient was unconscious while the defendant care providers were in control of what occurred and what was documented. None of the parties involved testified anything went wrong, yet according to the patient's expert, the outcome indicates something must have gone wrong. Similarly, none of the medical records indicated actions deviating from the applicable standards of care.

This is where the legal doctrine of res ipsa loquitor becomes involved. This doctrine provides a mechanism for patients in certain egregious situations. First, it relieves the patient of the duty to plead specific actions that caused the harm alleged. The patient also does not have to provide details of the standard of care the defendant allegedly breached. Instead, a patient need only complain the injury does not normally occur unless there is negligence — and the injury actually did occur. Second, at trial, the patient does not have to prove the specific actions that caused harm, or the standard of care that was breached.

Instead, the patient's case is indirect, as the patient is incapable of proving a direct cause-and-effect relationship. Typically, the patient proves the cause (e.g., a physician performing surgery perforated a bowel) and the effect (e.g., the patient suffered sepsis). Res ipsa loquitor forgoes this relationship because the patient cannot demonstrate the cause, and only knows the effect. In these circumstances, the patient relies heavily on expert testimony because experts can confidently state that such effects only happen when there is a cause, although the cause is unknown. Surgical errors are not uncommon, although they can produce a range of effects from minimal to fatal. Detailed, written reports following surgical procedures are important for physicians to protect themselves when a patient might later allege something went wrong. In the absence of a written report, it is more likely the patient will be able to find fault, whereas a detailed report helps convince a jury the physician adhered to the applicable standard and performed the actions described in the report.

Experts in medical malpractice actions are excessively commonplace — and, in fact, often determine the outcome of the action. In this case, the expert's testimony was precisely calibrated to support the res ipsa loquitor doctrine. The expert opined the patient's nerve injury "does not occur absent negligence," which directly addressed the necessary components under the applicable state law. Since the physician and care providers were in exclusive control of the patient during the surgery, and since the patient suffered permanent injuries during the surgery, the expert testified the actions of the defendants must have caused the injury. The court found this expert was sufficiently qualified to testify on these standards and procedures, and the testimony proved invaluable to reviving the patient's case on appeal. ■

REFERENCE

- Decided Oct. 28, 2021, in the Appellate Court of Illinois, Fourth District, Case Number 4-21-0038.