HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE SINCE 1979

INSIDE

Relias Media

From Relias

JANUARY 2021 Vol. 43, No. 1; p. 1-12

Cyberattack Almost Shuts Down Health System, Shows Need for Security

The recent cyberattack on a large health system shows the need for a robust security program, as well as how severely such an attack can affect healthcare operations.

Hackers breached the computer systems for the network of 400 hospitals and care centers across the United States and the United Kingdom, using ransomware that shut down nearly all of the computers, according to a statement by the health system. (*The statement is available online at: https://bit.ly/2IoCLQp.*)

The incident is believed to be one of the largest cyberattacks on a healthcare organization in U.S. history. Hospitals reported that clinicians were reduced to using pen and paper for some tasks as computer terminals shut down on their own, but the electronic health record (EHR) was not seized by the ransomware.

> HACKERS BREACHED THE COMPUTER SYSTEMS FOR THE NETWORK OF 400 HOSPITALS AND CARE CENTERS ACROSS THE UNITED STATES AND THE UNITED KINGDOM.

INTERPOL, the international law enforcement organization, issued a statement soon after the COVID-19 pandemic began saying there had been a significant increase in ransomware attacks against healthcare organizations. A month later, hackers infiltrated the computer systems of Fresenius, the largest private hospital operator in Europe.

The attack on the U.S. healthcare system shows that hackers are singling out hospitals as vulnerable targets,

Financial Disclosure: Author **Greg Freeman**, Editor **Jill Drachenberg**, Editor **Jonathan Springston**, Editorial Group Manager **Leslie Coplin**, Accreditations Director **Amy Johnson**, MSN, RN, CPN, and Nurse Planner **Maureen Archambault** report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study. Consulting Editor **Arnold Mackles**, MD, MBA, LHRM, discloses that he is an author and advisory board member for The Sullivan Group and that he is owner, stockholder, presenter, author, and consultant for Innovative Healthcare Compliance Group.

HEALTHCARE RISK MANAGEMENT™

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

GST Registration Number: R128870672

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

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

PHOTOCOPYING: No part of this newsletter may be reproduced in any form or incorporated into any information retrieval system without the written permission of the copyright owner.

Copyright © 2021 Relias LLC. *Healthcare Risk Management*™ *and Legal Review & Commentary*™ are trademarks of Relias LLC. The trademarks *Healthcare Risk Management*® and *Legal Review & Commentary*™ are used herein under license. All rights reserved.

says **Anthony Chadd**, senior vice president of security business development with Neustar, a technology and analytics company based in Sterling, VA.

"In the early days of the pandemic, some ransomware syndicates publicly announced they would stop all activity against medical organizations until a stabilization of the coronavirus situation," he says. "Clearly, that ceasefire has now ended."

Over the past few years, ransomware attacks have become easier to launch, and attackers increasingly are targeting healthcare organizations where cyber defenses may be less sophisticated and employees less savvy about how to spot threats, Chadd says. While providers typically have strong cybersecurity protections in place, many lack a mature cyber response plan. Even sophisticated organizations may not have the resources and expertise needed to initiate a successful recovery process, he says.

There have been several examples of attacks against small providers and practices that caused them to permanently close their doors after attackers encrypted and destroyed servers containing vital data and backup hard drives, Chadd notes.

"Attackers rightly recognize ransomware as an easy, effective way to garner financial gain. This dynamic is exacerbated by organizations that opt to pay the ransom — which perpetuates this cycle and leads to more attacks," he says.

Additionally, Internet-of-things (IoT) devices are increasingly finding their way into all levels of healthcare, he says. These devices, including smartphones, can link to computer systems and create vulnerabilities.

"Security and IT administrators must be aware of the risks they pose, and understand how the new threat vectors opened up by connected devices can potentially be exploited by attackers to harm the organization," Chadd says. "The IoT has essentially been built on top of infrastructure that is fundamentally vulnerable to cyberthreats, because the internet was not initially created with security in mind. To avoid becoming a target, healthcare organizations must be proactive in their approach to cybersecurity and make it a priority to safeguard all IoT-based systems."

The loopholes are numerous, and many healthcare organizations lack the resources and manpower required to manage the kinds of dynamic threats they might face, Chadd says. They must manage a mix of IoT devices, cloud-based apps, and legacy systems that require regular patching and updating.

EXECUTIVE SUMMARY

A U.S. healthcare system recently was the victim of a cyberattack that hampered patient care. The attack is believed to be the largest such attack on a U.S. healthcare organization.

- Ryuk ransomware apparently was used.
- The attack did not shut down the system's electronic health records.
- Hackers increasingly are focused on healthcare organizations.

This often includes connected equipment running on Windows — devices that can be easily overlooked during an IT audit, Chadd says.

"Many organizations simply don't have the level of manpower required to oversee a robust cybersecurity program," he says. "Healthcare organizations face an uphill battle to protect themselves from the kinds of dynamic threats they face."

Russian Hackers Suspected

Ryuk, the ransomware allegedly used in the destructive attack on the U.S. healthcare system, typically is used by a handful of organized crime groups out of Russia, says **Caleb Barlow**, CEO of CynergisTek, a healthcare information security company based in Austin, TX. In many ways, it looks like this attack was a near-miss that could have been a lot worse, he says.

"It does not appear that the EHR was directly impacted in the attack but rather just their IT systems. I suspect that their EHR is outsourced to Cerner," Barlow says. "I would view this as a failed attempt if the adversary was not able to take down the EHR, which is the primary target in healthcare."

A key point, Barlow says, is that a foreign criminal organization knowingly targeted a major U.S. healthcare system in the middle of a pandemic with full knowledge that they may have a direct impact on patient care and people's lives across hundreds of medical facilities.

"This is only a few weeks after the first confirmed death of a patient due to a ransomware incident in Germany. The point we have to look at here is adversarial intent," he says. "The adversary in this case likely knew the size of the system they were targeting, the number of facilities, and the likely impact it could have if they were successful in locking out their EHR."

Barlow says the attackers may be so insulated from the reach of law enforcement and intelligence agencies that they felt confident they could take down a target the size of the affected U.S. healthcare system without repercussions.

"Or did they first check in with their local government knowing that if they completely locked up hundreds of U.S. hospitals for an extended period of time, it could result in political pressure?" Barlow says. "Either situation is a cause

Ransomware Is Fast, Need to Practice Response

Ransomware can act with amazing speed, says **John Ford**, cyber strategist with IronNet, a cybersecurity company based in McLean, VA. He once worked with a company that was attacked with ransomware, and more than 1,000 machines were affected in less than 90 seconds, he says.

"You have to be able to get systems back up and running. So if it goes on for a very long time like a week or two, that's an indicator that the backups were an issue," he says. "The recent attack shows that you must always stress the importance of staff members not opening any mail that could be a phishing attempt."

"With COVID, people are very overworked and stressed. When you take that kind of environment and present a ransomware attack, there is a huge risk someone is going to let their guard down and let that attack into the hospital system," Ford says. "Before you know it the computer terminals are shutting down, the radiology units, everything is going offline, and people can't do their jobs."

Ford recommends tabletop exercises to let hospital leaders run through the protocols for how to respond to such an attack in real time, looking for any uncertainty or practical problems in executing it.

"Ransomware is not just about the security team. It's about everyone else affected by the ransomware and how they try to do their jobs while you sort this out," Ford says. "They have to know what to do."

Ford says he expects to see a great deal more of the ransomware attacks that hit the U.S. healthcare system.

"It's a perfect business model for the bad guys. There is very little barrier to entry, and limited or no competition," Ford says. "You don't need a phenomenal skill set, and the return on investment is significant. We followed one hacker who acquired the credentials for a U.S. healthcare provider for $300 in Bitcoin. Later that week they hit an entity that paid $150,000 in ransom. That's a pretty good return." ■

for concern and a significant escalation of what we have seen historically."

Double Layer Attack

Once the Ryuk payload has been successfully dropped and executed, it will encrypt the system's files and then demand a ransom fee to decrypt the victim's data, says **Bindu Sundaresan**, CISSP, CEH, CISM, director of AT&T Cybersecurity, based in San Mateo, CA.

"Ransomware attacks today have evolved to double extortion. Usually, the attacker would exfiltrate a copy of the data before encrypting them. This way, the attacker not only prevents the victim from accessing their data, but also keeps a copy of the data for themselves," Sundaresan explains. "In order to claim responsibility and pressure the victim during the negotiation process, the attacker will often release small portions of the data online. If the negotiation turns out badly, the attacker then publishes all of the exfiltrated data or sells them to third parties."

These attacks are essentially a combination of a ransomware attack and a data breach, she says. Organizations that are victims of this attack feel extremely helpless when hit by double extortion attacks because their compromised databases likely contain proprietary or secretive information they would have destroyed rather than published or sold, she says.

By releasing a small sample, it is easy for an attacker to imply they have your data, though difficult to prove forensically because most places do not have that layer of visibility, Sundaresan says. This puts on another pressure point. If the affected organization has implemented a data loss prevention (DLP) solution, it can be easily validated that hackers have also downloaded the entire database.

Delivered in Phishing Emails

Ryuk ransomware is part of the TrickBot's malware strain, says **Mike Puglia**, chief strategy officer with Kaseya, a cybersecurity company based in Miami. Major efforts from both the private and public sectors were used to disrupt TrickBot operations in the lead-up to the 2020 general election. Microsoft obtained an order in the Eastern District of Virginia in October that gave the tech giant control over the TrickBot botnet, a global network it describes as the largest in the world, Puglia says. The U.S. Cyber Command also conducted operations against TrickBot to damage and disrupt the organization itself as well as the group's cybercrime as-a-service operation.

Ryuk ransomware is often delivered through phishing emails, Publia says. The continued prevalence of ransomware attacks through phishing underscores just how critical it is for both the public and private sectors to invest in comprehensive integrated email security solutions combined with cybersecurity training to ensure that employees are adequately prepared to spot suspicious emails, he says.

"While TrickBot operations may be hampered for now, the organization — and others like it — will continue to find new ways to launch cyberattacks, taking advantage of unhardened networks and untrained employees as their way in," Puglia says.

It appears the ransomware disabled antivirus programs and spread rapidly, says **MJ Kaufmann**, Cyber Security Specialist at Saviynt in El Segundo, CA. Based on prior Ryuk attacks, it likely started out distributed via a phishing email or infected software. From there, Ryuk sets up as a root kit, allowing bad actors to actively push it throughout the network, which is one reason for the attack's massive scale, she says.

"If the health system lacked sufficient network segmentation that prevented easily shutting down the infected portions selectively, that might explain the widespread outage," Kaufmann says. "Another possibility is they lacked the intelligence-gathering capabilities to unquestionably identify infected portions so they could be isolated; thus, a mass shutdown might have been prevented."

Other healthcare organizations and systems can learn from this example and implement security and identity protocols to prevent and combat ransomware attacks, Kaufmann suggests. The best way to combat such an attack is to start with heuristic-based anti-malware software on endpoints to detect and shut down questionable behavior early, she says.

"Combine this with a zero-standing privilege environment where there are no standing superusers or administrators to take advantage of make attacks like this much more challenging to undertake," she advises.

Seeing Hospitals as Good Targets

Cyber thieves are attacking healthcare institutions more often and are acquiring more valuable data than in the past, says **Steve Tcherchian**, chief information security officer at XYPRO, a

cybersecurity analytics company in Simi Valley, CA.

When the price of a stolen credit card dropped precipitously because the black market was flooded with them, hackers found a new target in the healthcare industry, he says. On the whole, the healthcare industry has an aging infrastructure that is less resistant to hacking, and industry tends to adopt security precautions more slowly than other potential targets, Tcherchian says.

He says that many medical data breaches are now as big as the largest retail breaches, and medical records can be 10 times as valuable as credit cards on the black market.

A patient's medical history can be the key for a hacker to commit medical identity theft and submit fraudulent insurance claims, which have the potential for big payouts, Tcherchian says. According to IBM Security's 2020 data breach cost report, the average cost of a healthcare data breach is $7.13 million. Cyber thieves also may use the information to purchase prescription drugs and resell them online, he says.

(*See the story in this issue for tips on how to protect your organization from cyberattacks.*)

Resistance to Blocking

Hospitals are extremely susceptible to ransomware and other types of cybercrime because they are inherently so open to exchanging files, connecting with thousands of doctors' offices and hospitals constantly, says **Jack B. Blount**, president and CEO of Intrusion, a company providing cybersecurity services in Plano, TX. For this same reason, they often have been the most resistant to any kind of blocking of connections for fear that a critical piece of data — such as

Four Pillars of Cybersecurity Can Help Prevent Trouble

To implement a cybersecurity solution, one needs to understand the four pillars of cybersecurity, says **Gary Salman**, CEO of Black Talon Security in Katonah, NY.

The pillars are Cybersecurity Awareness Training, Cybersecurity Audit, Vulnerability Scanning, and Penetration Testing.

Under the HIPAA security rule and many states' breach laws, organizations are required to implement cybersecurity awareness training for every employee in the organization. This is a comprehensive training that helps leaders and employees understand and identify threats that present themselves through email, internet, and lack of standard operating procedures related to password and access point protection for the network, Salman says.

The second pillar is a cybersecurity audit. During this audit, a cybersecurity company will work closely with the organization and IT company to understand, from a holistic perspective, the entire network and IT infrastructure, Salman says. An audit will uncover vulnerabilities in the infrastructure and procedures that may allow someone to gain access to data, he says.

The third pillar is vulnerability scanning. This can be broken down into two components, Salman says. A HIPAA scan is a very basic scan that examines the network for vulnerabilities that may result in unauthorized access or the exposure of patient data, ultimately causing a HIPAA violation. It is not designed to find vulnerabilities in the network, such as improperly configured computers, devices, or servers, Salman says.

"On the other hand, a vulnerability scan is very comprehensive and is designed to find the unlocked doors and windows on your network that a hacker would use to exploit data," he says.

The final pillar of cybersecurity is a penetration test, also known as a Pen test. This is performed by one of the cybersecurity company's ethical hackers, known as white hat hackers. The goal is to try to break into the network using the same tools, techniques, and protocols a criminal would use, Salman says. Once in, hackers will try to exploit various protocols and technologies to gain access to a workstation or server.

"By following the four pillars of cybersecurity and compliance, you can feel confident that you have done everything to comply with federal, and often state, laws and that your network is as secure as possible," Salman says. "Nothing is ever 100% secure, but these best practices will significantly improve your security posture." ■

SOURCE

- **Gary Salman**, CEO, Black Talon Security, Katonah, NY. Telephone: (800) 683-3797.

patient information or an X-ray — will be blocked in error, he says.

With this resistance to cybersecurity, organizations increase their exposure to cybercrime and become the target of constant breaches, Blount says. The healthcare industry needs to understand that the internet is flooded with cyberattacks 24 × 7 × 365, he says.

"It is normal for a hospital to get 10,000 to 50,000 attacks a day. Many, probably most, of those attacks get onto their network and then begin analyzing the network to determine what and when they want to attack," he says. "The only way to stop them is by implementing a solution that uses real-time artificial intelligence to inspect every packet of data coming onto or attempting to exit a network. This can stop thousands of attacks every day."

Hospitals often have aging infrastructure, systems that are difficult to patch, and huge attackable surface areas given the number of people who need to access sensitive data, says **Satya Gupta**, co-founder and chief technology officer at Virsec, in San Jose, CA.

"Ransomware and related attacks continue to be a ticking time bomb for many organizations, especially in healthcare. Unfortunately, ransomware is often viewed too simply as an endpoint problem," Gupta says. "Even with the best security on devices and user training, endpoints will always be porous. We need to focus much more on the target of ransomware — the applications, workloads, and servers that contain sensitive data that can be corrupted or stolen."

Hospitals should strive for greater visibility into what is happening at the workload level in real time, to make them much more resilient and self-defending, Gupta says.

Perimeter security solutions inevitably fall short against increasingly sophisticated ransomware attacks, says **Jon Toor**, chief marketing officer with Cloudian, a data storage and security company based in San Mateo, CA. To truly safeguard themselves, organizations must instead protect data at the storage layer, he says.

"The easiest way to do this is to keep a backup data copy on immutable storage. Once written, the backup cannot be changed or deleted for a specific period. This prevents malware from being able to encrypt the data and lock the victim out," Toor says. "If a ransomware attack occurs, organizations can restore an unencrypted copy of the data via a simple recovery process."

> "RANSOMWARE AND RELATED ATTACKS CONTINUE TO BE A TICKING TIME BOMB FOR MANY ORGANIZATIONS, ESPECIALLY IN HEALTHCARE."

Multiple backup vendors now support this feature, Toor notes.

Increasing Attacks in Healthcare

Cyberattacks are increasing in the healthcare sector due to business practices and organizational trends, says **Nicole Bucala**, vice president of business & corporate development, strategy, and operations at Illusive Networks, a cybersecurity firm based in Tel Aviv, Israel, with an office in New York City. Acquisitions and consolidations create security gaps as entities work to unify their IT networks and applications, she says.

Smart medical devices and electronic record systems introduce new vulnerabilities and increase the attack surface, Bucala says. Of course, the rise of remote work has also increased the attack vector.

Bucala notes that the U.S. health system was affected by the cyber-attack for several days. Treatment was difficult because the medication system for the hospital was internet-based. Reverting to pen and paper was not just arduous and inefficient; it also increased the potential for mistakes.

The recent incident in Germany illustrates how bad a ransomware attack can be in the healthcare industry, Bucala says. A ransomware attack hit the University Hospital in Dusseldorf, although it appears to have been meant for a local university. The hospital systems crashed after malicious software encrypted 30 servers, and an extortion note was left on one of them. A patient died after they were rerouted to an alternate hospital, causing possibly the first documented case of a ransomware-related death, Bucala says.

Advanced ransomware threats (ARTs) are the biggest concern of all, Bucala says. ARTs combine advanced persistent threat (APT) techniques with ransomware techniques. Like an APT, sophisticated ransomware attackers target and navigate to carefully selected strategic assets on the network that hold business-critical information, she explains.

"Attackers then take those assets hostage using advanced evasive ransomware techniques, massively

How to Defend Against Ransomware Attacks

Steve Tcherchian, chief information security officer at XYPRO, a cybersecurity analytics company in Simi Valley, CA, recommends these steps to prevent ransomware attacks:

• **Educate staff.** They are the first line of defense. No amount of technology or money thrown at this problem will be a substitute for a properly trained staff. A single unintended click on a link in an email can sink the whole ship.

• **Inventory and categorize technology assets.** Understand what happens if certain technology assets, such as file servers or financial data, become unavailable or are compromised.

• **Understand notification obligations.** Do not exacerbate the problem by not complying with laws when a breach occurs.

• **Create an incident response plan.** Make sure everyone understands their roles so people are not panicking, looking for guidance, or stepping on each other's toes.

• **Back up everything.** Often. Make sure you have healthy backups you can test and validate on a weekly basis. It is not enough for the IT guy to receive an email notification once a week saying "backups were successfully completed." Is the organization backing up the right data? Have the data that need to be backed up changed? Can those data be restored successfully? How long will it take? These are questions any small business should ask and be able to answer before an attack.

• **Create multiple, different backups.** For small businesses, there are a variety of cloud backup providers to choose from. Do not back up data on the same computer on which data live, or on an external network or USB drive in someone's office, which is susceptible to the same attack, fire, or theft.

• **Use antivirus and malware software.** They work.

How an Attack Happens

Christopher Gates, principal system security architect with Velentium, a cybersecurity company in Katy, TX, describes how a typical cyberattack of the Ryuk variant unfolds:

1. A user opens a phishing email with infected files, containing obfuscated VBA code.
2. The VBA code is downloaded and executes the Emotet trojan from a hacked WordPress site.
3. Emotet "phones home" to its command and control servers.
4. Emotet sends massive amounts of spam with a URL that links to the hacked WordPress sites, looking for others to infect.
5. After some time (months), Emotet installs the TrickBot trojan from those hacked WordPress sites to collect sensitive data, including passwords, cookies, and SSH keys.
6. TrickBot spreads itself across the health system network.
7. TrickBot eventually opens a reverse shell for the attackers.
8. Using the reverse shell (and probably an exploit toolkit called "Empire"), the attackers install the Ryuk ransomware.
9. Ryuk starts encrypting and renaming files across the network with the .ryk filename extension.

To prevent this kind of attack, Gates advises regularly training employees to identify phishing emails and phishing social media and create a policy and a mechanism for employees and end-users to report suspicious messages. ■

SOURCE

- Christopher Gates, Principal System Security Architect, Velentium, Katy, TX. Email: nextstep@velentium.com.

disrupting hospital operations and saying they will stop only in exchange for a very high fee," Bucala says. "Organizations without proper ART protection have no choice but to pay the fee to avoid further disruptions, loss of money, and even loss of life."

These threats are serious, but they are not insurmountable, she says. To beat an attacker, think like an attacker, Bucala advises. When a security team thinks like an advanced attacker, it can know what the attacker is after and can focus on those assets. Every healthcare organization needs to be able to view the attack landscape, map attack

pathways, and know where the high-risk critical assets are, which will be fundamental for building a strategy for pre- and post-breach penetration, she says.

IT security teams at healthcare organizations need to focus on active detection to minimize, or even prevent, damage from a ransomware attack. This should include the ability to detect lateral movements within the network, Bucala says.

Deception technology is a category of security tools designed to detect attackers who already are in the network and prevent them from doing damage, Bucala explains. It works by distributing deceptions that mimic genuine IT assets throughout the network. Instead of relying on traditional signatures, deception technology alerts are generated by real attacker movements within a network, she says.

"The IT team will be able to see, in real time, any malicious lateral movement that is happening on the network and can mitigate the attack, protecting the computer systems that literally keep people alive," Bucala says. ■

SOURCES

- **Caleb Barlow**, CEO, CynergisTek, Austin, TX. Telephone: (512) 402-8550.
- **Jack B. Blount**, President and CEO, Intrusion, Plano, TX. Telephone: (972) 234-6400.
- **Nicole Bucala**, Vice President of Business & Corporate Development, Strategy, and Operations, Illusive Networks, New York City. Telephone: (844) 455-8748.
- **Anthony Chadd**, Senior Vice President of Security Business Development, Neustar, Sterling, VA. Telephone: (855) 898-0036.
- **John Ford**, Cyber Strategist, IronNet, McLean, VA. Telephone: (443) 300-6761.
- **Satya Gupta**, Co-founder and Chief Technology Officer, Virsec, San Jose, CA. Telephone: (877) 213-3558.
- **MJ Kaufmann**, Cyber Security Specialist, Saviynt, El Segundo, CA. Telephone: (310) 641-1664.
- **Mike Puglia**, Chief Strategy Officer, Kaseya, Miami. Telephone: (877) 926-0001.
- **Bindu Sundaresan**, CISSP, CEH, CISM, Director of AT&T Cybersecurity, San Mateo, CA. Telephone: (650) 713-3333.
- **Steve Tcherchian**, Chief Information Security Officer at XYPRO, Simi Valley, CA. Telephone: (805) 583-2874.
- **Jon Toor**, Chief Marketing Officer, Cloudian, San Mateo, CA. Telephone: (650) 227-2380.

Structure, Time Limit Optimize Results from Safety Huddles

Indiana University Health in Indianapolis is using a carefully structured adverse event huddle across its entire health system to encourage hospitals to share information about patient safety.

About three years ago, the 16-hospital network began scheduling a 30-minute, systemwide phone call once a week to discuss patient safety issues, explains **Michele S. Saysana**, MD, vice president of patient safety.

"Each hospital shares whether there have been any adverse events or near misses in the hospital, and any lessons learned from them. Sometimes, they have already done a deep dive into what happened, and sometimes, they have not," Saysana says. "It improves transparency among our hospitals, but the real purpose is that if it could happen in one hospital, it could probably happen anywhere else. We want to share that information as quickly and as broadly as possible."

The adverse event huddle calls are attended by the risk managers, chief medical officers, chief nursing officers, and quality leaders of each hospital, along with the chief medical officer and chief nursing offer of the system, and Saysana representing system-level patient safety. The risk manager at each hospital typically prepares information for the call and leads the discussion for events at that facility, she says.

EXECUTIVE SUMMARY

A health system is using weekly adverse event safety huddles to improve transparency. Each of 16 hospitals shares information about patient safety incidents.

- The meetings have a strict 30-minute time limit.
- A structured format ensures efficiency.
- Hospitals report on how they have addressed earlier incident reports.

Initially, there was reluctance about sharing information that might be perceived as negative, with hospital leaders fearing that the disclosure of an adverse event or near-miss might discourage other hospitals from transferring patients, Saysana says. There also was a practical challenge in simply scheduling the weekly call.

With so many busy hospital leaders involved, it was impossible to negotiate a time that worked well for everyone.

"We finally picked a day and time and just told everyone it's Thursdays at noon. No time was going to work for everyone so we had to choose," she says. "We committed to the meeting lasting only 30 minutes and ending at 12:30 p.m. sharp, so that helped people with their schedules."

The strict time limit is made possible by using a formal structure for the meetings and a facilitator. The meeting facilitator calls on each region in the health system to see if any hospital there has an incident to report. Any hospital that will be reporting sends a written summary to the meeting participants beforehand so they can follow along.

Meeting participants were taught to provide the information about a patient safety incident in a succinct way. At this point in the meeting, there was little to no discussion among the participants, Saysana says. Discussions were held to the end of the meeting to ensure there is time for the presentations.

"We encourage them to reach out to each other after the meeting," Saysana says. "The goal is to get these incidents out on the table so that everyone knows, and then we can follow up appropriately outside the time restrictions of this meeting."

After the weekly meetings were well-established, the format was modified. On the first and third Thursdays, regions bring forward events. On the second and fourth Thursdays, all the regions share what they have done to follow up on that information, she explains.

At that point, there was more time for discussion in the meetings because participants had more experience with what information to bring, how to present it, and the most effective ways to talk about possible responses, Saysana explains.

The regular meetings were paused during the COVID-19 outbreak because of the pressure hospitals were under, but Saysana expects them to resume soon. The patient safety huddle model was modified for daily huddles, with the incident command structure about COVID-19 issues, such as how to move patients around in response to staffing and resource shortages, Saysana says.

"The safety huddles helped us learn to work better and have more transparency among our institutions. That translated well when we needed to do the same thing to help each other work through COVID-19," she says. "We are now bringing harm back into these meetings with our CMOs and CNOs, because at the same time we're addressing COVID-19, we want to be sure we are staying vigilant about other patient safety issues." ■

SOURCE

- **Michele S. Saysana**, MD, Vice President of Patient Safety, Indiana University Health, Indianapolis. Telephone: (317) 948-2700.

OCR Seeking Ways to Improve HIPAA, Respond to Value Concerns

The Office for Civil Rights (OCR) is asking the public for ways to modify HIPAA regulations, specifically to drive cost savings and value, notes **Jeffrey P. Drummond**, JD, partner with Jackson Waller in Dallas. The changes are intended to help HIPAA mesh better with coordinated care platforms and improve care coordination, he says.

HIPAA is naturally obstructive to care coordination, Drummond says. "Any efforts at care coordination naturally assume ready exchange of patient information among providers, payors, and others involved in the care of the patient, or the patient population, while HIPAA's focus on privacy and security generally limits information sharing," he says. "However, as currently established, HIPAA does allow for such sharing of patient medical records, as long as the purpose of the disclosure is treatment, payment, or general healthcare operations."

In most cases where information would or could be shared to assist with care coordination, HIPAA would allow it, Drummond says. The major problem is that too many people in the healthcare industry do not understand HIPAA and are afraid of it, Drummond says, so they refuse to share information even though HIPAA would allow it.

Another major problem is that given the combination of the Facebook and other social media

platform privacy issues all over the news, as well as the daily reports of major breaches of personal and medical information, many people are too afraid their medical record privacy will be abused, he says.

"People fear for their privacy, so they don't want their information released, even though releasing the information in an appropriate manner would actually improve their healthcare and the overall cost of healthcare," Drummond says.

Those problems cannot be fixed by changing HIPAA, Drummond says, because as currently structured, HIPAA already should work to allow appropriate information exchange for care coordination and value-based healthcare.

"I do not see any major changes being made to HIPAA," Drummond says. "However, given the push for regulatory change, and the need to be seen to be doing something, particularly something de-regulatory, I would expect some tinkering around the edges."

This is what Drummond expects in future changes to HIPAA:

- minor tweaks to the definition of "healthcare operations" to clarify and possibly expand the ability to share protected health information for population health, emergencies, and value-based care initiatives;
- minor clarifications regarding "personal representatives" and when parents are (or are not) treated as such;
- specific language (more likely guidance than changes to the actual text of the regulations) addressing uses and disclosures in the mental health and substance abuse arena;
- revisions to the "accounting of disclosures" requirements (proposed regulations have been languishing there for years) to streamline the process by eliminating much of the requirement (contrary to the emphasis of HITECH to increase the requirement);
- finalization of the rule allowing individuals to share in the fines levied by OCR for a HIPAA breach;
- specific language addressing when a ransomware attack (or similar technology-driven incident) is a reportable breach.

Some commentators will ask for removal of the requirement to have patients sign to acknowledge receipt of the Notice of Privacy Practices when they first go to their doctor, Drummond says, but he does not think that actually will occur.

"It would definitely remove a noticeable burden on both providers, who have to print out notices, ask for signatures, and keep track of them. Ultimately, that's a small burden to make sure that providers actually provide the notice, and patients have an opportunity to think about how their information is going to be used and disclosed," he says. "Ultimately, I think they'll leave it in place as is." ■

SOURCE

- **Jeffrey P. Drummond**, JD, Partner, Jackson Waller, Dallas. Telephone: (214) 953-5781. Email: jdrummond@jw.com.

Annual Physician Liability Survey Reveals Hardening Markets

Medical professional liability claims are stable, but professional liability loss costs for hospitals and physicians are estimated to increase by 3% annually over the next few years, according to the latest Aon/ASHRM Hospital and Physician Professional Liability Benchmark Analysis.

Hardening markets are prompting healthcare organizations to maintain higher retentions, says **Kanika Vats**, FCAS, MAAA, MBA, director and actuary, and healthcare practice leader in the Global Risk Consulting, Commercial Risk Solutions division of Aon in New York City.

The trend of a 3% rise in the severity of malpractice claims, measured by the average cost of resolution, is higher than the 2% rise seen in recent years, Vats says.

"We think one of the key drivers for this has been the large jury settlements taking place in the last few years. On the frequency side of things, hospitals and providers have been doing a good job of managing the claims frequency. As a result of those efforts we see frequency remaining flat for the fifth year in a row," Vats says.

COVID-19 may influence those numbers in the near future, she says. Courts were closed for months in 2020, delaying the progress of many liability claims, Vats notes, and that could create a bubble of fewer verdicts and settlements. Criminal cases also were delayed. Once courts resumed litigation, the criminal cases took priority over civil cases, she explains.

That could affect the expected 3% rise in professional liability loss

costs for hospitals and physicians, she says.

"There was a backlog of civil cases, so that could have an effect on the data we will see from professional liability claims that are taken to trial," she says.

From 2016 to 2019, there was a 50% increase in settlement amounts to some high-severity cases with a jury verdict of $5 million or more, Vats says. To combat that increase, one strategy is for the hospital to provide a settlement offer that is a fair value during the jury trial process and stick with it, she says.

"Defend that number vigorously. That number should be tied into the reasonable economic damage argument," Vats says. "We've also heard of defendants finding success with offering high-low agreements to cap the minimum and maximum."

(*The report is available for purchase online at: https://aon.io/3mygWNa.*) ■

SOURCE

- **Kanika Vats**, FCAS, MAAA, MBA, Director and Actuary, Healthcare Practice Leader, Global Risk Consulting, Commercial Risk Solutions, Aon, New York City. Telephone: (212) 441-1425. Email: kanika.vats.@aon.com.

Telemental Health Survey Finds Increased Risk of Fraud

The expansion of telehealth services brings more risk of fraud and a greater need for internal compliance programs, according to the 2020 Telemental Health Laws survey from Epstein Becker Green in Washington, DC.

In its fifth year examining state telemental health laws, regulations, and policies, the firm found that the COVID-19 pandemic has put pressure on lawmakers to increase access to telemental health services, while also finding greater potential for fraud. (*The full report is available online at: https://bit.ly/32ijff5.*)

State laws are changing rapidly regarding the use of telehealth services, says **Amy Lerman**, JD, an attorney with Epstein Becker Green and the main author of the report. That increases the risk of noncompliance as organizations work with providers across state lines, she says.

"Within many of the states, for instance, there are evolving approaches to remote subscribing. Tracking issues like that can be challenging to keep track of what your licensed professionals can do in that area," she says "We don't see as often that states remove these laws, with it being more common to provide positive guidance. But there are nuances, especially with mental health services. A mental health provider may need to follow more requirements and have more obligations than other providers."

Fraud is another concern as the use of telemental health services increase, Lerman says.

"The enforcement bodies are watching, so it more important now than ever to make sure you are doing everything in the right way. You need to know if you can do in Texas what you are doing in Pennsylvania," she says. "It matters because there is enforcement activity ongoing. The magnitude of it is very significant, especially from a risk perspective." ■

SOURCE

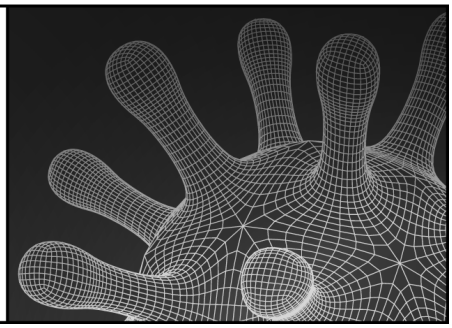
- **Amy Lerman**, JD, Epstein Becker Green, Washington, DC. Telephone: (202) 861-1832. Email: alerman@ebglaw.com.

10 CME/CE Credits

New from Relias Media

The COVID-19 Handbook: Navigating the Future of Healthcare provides a fact-based approach to address multiple aspects of the COVID-19 pandemic, including potential therapeutics, the effect on healthcare workers, and the future of healthcare in a post-COVID world.

Visit ReliasMedia.com



HEALTHCARE RISK MANAGEMENT™

EDITORIAL ADVISORY BOARD

Arnold Mackles, MD, MBA, LHRM
President, Innovative Healthcare Compliance Group, Palm Beach Gardens, FL

Maureen Archambault, RN, MBA, HRM, CPHRM, FASHRM
Senior Vice President, Chief Risk Officer
Prospect Medical Holdings
Los Angeles

Leilani Kicklighter, RN, ARM, MBA, CPHRM, LHRM, Patient Safety & Risk Management Consultant, The Kicklighter Group, Tamarac, FL

John C. Metcalfe, JD, FASHRM
J.C. Metcalfe & Associates
Los Alamitos, CA

William J. Naber, MD, JD, CHC, Medical Director, UR/CM/CDI, Medical Center & West Chester Hospital, Physician Liaison, UC Physicians Compliance Department, Associate Professor, University of Cincinnati College of Medicine, Cincinnati

Grena Porto, RN, ARM, CPHRM, Vice President, Risk Management, ESIS ProCLaim Practice Leader, HealthCare, ESIS Health, Safety and Environmental, Hockessin, DE

R. Stephen Trosty, JD, MHA, CPHRM, ARM, Risk Management Consultant and Patient Safety Consultant, Haslett, MI

M. Michael Zuckerman, JD, MBA, Assistant Professor and Academic Director Master of Science, Risk Management & Insurance, Department of Risk, Insurance & Healthcare Management, Fox School of Business and Management, Temple University, Philadelphia

Interested in reprints or posting an article to your company's site? There are numerous opportunities for you to leverage editorial recognition for the benefit of your brand. Call us: (800) 688-2421. Email us: reliasmedia1@gmail.com.

Discounts are available for group subscriptions, multiple copies, site licenses, or electronic distribution. For pricing information, please contact our Group Account Managers at groups@reliasmedia.com or (866) 213-0844.

To reproduce any part of Relias Media newsletters for educational purposes, please contact The Copyright Clearance Center for permission: Email: info@copyright.com. Web: www.copyright.com. Phone: (978) 750-8400

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. **What does Anthony Chadd, senior vice president of security business development with Neustar, a technology and analytics company based in Sterling, VA, say is one lesson from the recent ransomware attack on a U.S. health system?**

   a. Hackers are singling out hospitals as vulnerable targets.
   b. Hackers are shying away from the healthcare industry when seeking targets.
   c. Hospitals are becoming much more resistant to cyberattacks.
   d. Hospitals are vulnerable to attacks, but hackers find little of value when they are successful.

2. **Which of the following statements is true regarding the weekly adverse event huddle phone calls used by Indiana University Health in Indianapolis?**

   a. They are strictly limited to 30 minutes per hospital.
   b. They are strictly limited to 30 minutes total.
   c. Only hospitals with an event to report attend the weekly meeting.
   d. Each hospital is required to report at least one event per meeting.

3. **What is one finding from the latest Aon/ASHRM Hospital and Physician Professional Liability Benchmark Analysis?**

   a. Professional liability loss costs for hospitals and physicians are estimated to fall by 3%.
   b. Professional liability loss costs for hospitals and physicians are estimated to grow by 3%.
   c. Hardening markets are leading healthcare providers to maintain lower retentions.
   d. Softening markets are leading healthcare providers to maintain higher retentions.

4. **According to Mike Puglia, chief strategy officer with Kaseya, a cybersecurity company based in Miami, how is the Ryuk ransomware often delivered?**

   a. Phishing emails
   b. Infected hard drive installations
   c. Portable thumb drives
   d. Visits to infected websites

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

Complications from Gastric Bypass Surgery Result in Brain Injury, $14.1 Million Award

*By **Damian D. Capozzola**, Esq.*
The Law Offices of Damian D. Capozzola
Los Angeles, CA

***Jamie Terrence**, RN*
President and Founder, Healthcare Risk Services
Former Director of Risk Management Services (2004-2013)
California Hospital Medical Center
Los Angeles, CA

***Elena N. Sandell**, JD*
UCLA School of Law, 2018

News: A patient underwent gastric bypass surgery, but suffered permanent brain damage because of post-surgery complications and requires around-the-clock care for the rest of her life. The patient sued, alleging that the physician who performed the procedure failed to recognize that she was suffering from a severe thiamine and vitamin B1 deficiency, which led to her injuries. A jury awarded a $14.1 million verdict. The defendant physicians appealed, but the appellate court affirmed the verdict.

Background: In November 2011, a woman underwent gastric bypass surgery. Less than one month later, she began experiencing complications, including nausea and vomiting, which she immediately reported to the physician who performed the procedure. According to the patient, her symptoms worsened when she attempted to eat solid food, but liquids were not problematic. The physician suspected a stricture occurred as a result of the bypass surgery; in January 2012, the physician performed an outpatient dilation procedure.

THE PATIENT SUED, ALLEGING THE PHYSICIAN WHO PERFORMED THE PROCEDURE FAILED TO RECOGNIZE THAT SHE WAS SUFFERING FROM A SEVERE THIAMINE AND VITAMIN B1 DEFICIENCY.

Two days after the second procedure, the patient was treated for dehydration; the next day, she went to the emergency department (ED) complaining of vomiting. On admission to the hospital, she provided a history of the prior procedures and indicated she had lost 100 pounds during the six weeks following the procedures. A computed tomography (CT) scan was performed in the ED, and the results suggested the patient was suffering from an esophageal rupture. She was admitted to the intensive care unit (ICU) and subsequently diagnosed with pancreatitis and dehydration. At this time, she was alert and responsive, and there was no indication she was suffering from any deficit of movement in her extremities.

A few days after admission in the ICU, another physician took over the patient's care. She had difficulty walking even when she was assisted by nurses, and she complained of a tingling sensation in her fingers and tightness in her shoulder. Additionally, the patient's vomiting had not subsided, she had lost control of her bowels, and although she was awake, she would not respond to the physician's questions, leading the physician to question if she was depressed. During the next week, the patient did not receive any food or liquid by mouth. Although providers attempted to administer fluids by mouth, the patient was not able to tolerate them. A second nutritional assessment was performed, and total parenteral nutrition (TPN) was suggested again. However, TPN was not started, and the patient continued to suffer from dizziness, vomiting, and Trendelenburg gait, which occurs in people with weakness in their pelvic muscles.

Approximately a week later, the patient was discharged

with orders for TPN administration at home. The diagnosis recorded on her discharge chart identified intractable nausea and vomiting, obesity, and obstructive sleep apnea. During her hospital stay, the patient never received supplemental thiamine or vitamins. Furthermore, the TPN order did not include thiamine, only glucose and other nutrients. Three days after discharge, the patient was re-admitted to the hospital. Her condition had deteriorated significantly and was marked by confusion and mental decline. During this admission, the patient was placed on a ventilator.

The patient was diagnosed with Wernicke's syndrome, a condition causing encephalopathy due to severe thiamine deficiency. However, by the time the patient was diagnosed, her condition had worsened significantly and had progressed to Korsakoff syndrome, an irreversible condition that causes permanent brain damage. As a result of the untimely diagnosis, the patient suffered permanent brain injury and will require around-the-clock care for the rest of her life.

The patient sued the physician who performed the surgery as well as those who provided care after. The defendant physicians denied liability and wrongdoing. A jury found for the patient and awarded $14.1 million, which was upheld despite an appeal by the defendant physicians.

What this means to you: This case reveals the potential significant liability and injuries that can arise because of a delayed diagnosis, a common form of medical malpractice. Through the course of the litigation, there were three primary issues surrounding the delayed diagnosis.

First and foremost, the defendant care providers argued that the patient did not provide sufficient evidence to prove a diagnosis of Wernicke's syndrome. The defendant physicians argued that based on the patient's clinical charts and their observations, it was unclear whether the patient even suffered from this condition. Instead, the care providers argued that the patient's injuries were caused by a stroke she allegedly had suffered at some point after her first hospitalization. However, one of the defendant physicians admitted during testimony that he was not aware of the existence of Wernicke's syndrome, especially as a possible complication for patients who had undergone gastric bypass surgery. Furthermore, one of the defendants also acknowledged that at the time he prescribed TPN, he was unaware that prescribing glucose without a thiamine supplement would further decrease the patient's thiamine levels because thiamine metabolizes glucose.

According to the patient's expert, the symptoms of Wernicke's syndrome include vomiting, nausea, and low thiamine levels. Based on this information, the expert opined that the defendant physicians breached the standard of care by failing to accurately and promptly diagnose the patient and to intervene before the harm became irreparable. The patient introduced the results of her blood work, which was taken immediately prior to her discharge from the hospital. The blood tests revealed a severe vitamin B1 deficiency and very low thiamine levels. Based on this evidence and on the known history of gastric bypass surgery, the patient argued that the defendant physicians should have known to prescribe thiamine supplements — and the failure to do so constituted malpractice. Although the defendant physicians offered the alternative cause of a stroke, they failed to produce sufficient evidence to support that theory. On the contrary, all the evidence presented by the patient through her experts, as well as her medical records, supported the theory that had the care providers timely diagnosed the condition, the patient would not have sustained permanent brain damage.

Bariatric surgery requires great skill and expertise in the metabolic ramifications of diverting and limiting the digestion of nutrients in the human body. It is a delicate balance with which many patients struggle, and some succumb to the various complications that commonly arise. Protracted nausea or uncontrollable diarrhea can wreak havoc on the body's electrolyte balance, glucose levels, blood pressure, and other vital functions. Only a physician who specializes in bariatrics should manage these patients both pre- and postoperatively. TPN plus multivitamin injection is a common order. These two supplements support each other and the patient, who lacks nutrition and the ability to ingest nutrition normally. TPN is predominantly glucose with electrolytes and multivitamins, and often lipids should be given with it unless contraindicated. Fluid overload must be monitored and avoided, as well as the dumping syndrome or rapid loss of fluid in the gut, which may require an emergency response.

Other than the challenges to the alleged failure to diagnose, the defendant care providers raised arguments regarding the trial court's admission of evidence concerning a physician's loss of privileges at a hospital and about a settlement with the patient's daughter. While these presented legal challenges, neither were fruitful in this case to facilitate the care providers' positions. On the issue of the defendants' settlement with the patient's daughter, the court did order a subsequent hearing to determine what benefit, if any, the patient received from that settlement, which may offset her recovery on the jury verdict.

Finally, the court rejected the care providers' argument that the testimony of their expert concerning liability had been excluded erroneously and that the trial court erred in not allowing for periodic payments on the award for loss of earning capacity. In this case, the patient's injury was preventable and the care providers failed to introduce sufficient evidence to support their alternative theory. Most challenges raised by the care providers focused on procedural matters, and the court affirmed the $14.1 million award. Given the extent of the injury suffered, coupled with the clear thiamine and vitamin deficiencies that appeared from the patient's blood work, the court found sufficient evidence to support of the patient's claim and the jury verdict. ■

REFERENCE

Decided on Oct. 14, 2020, in the Texas Court of Appeals for the Fourth District, Case Number 04-18-00118-CV.

Defense Verdict Rejects $16 Million Demand, but 14-Minute Deliberation Gives Rise to an Appeal

News: A widow filed a malpractice action alleging a hospital's failure to evaluate the patient, which would have revealed extreme respiratory distress. The patient's death was caused by a lack of oxygen. Experts testified that if the patient had been placed on a ventilator, he would have had a significantly higher chance of surviving his condition, pneumonia. Following a seven-day trial, the jury rendered a defense verdict after a mere 14 minutes of deliberation. The plaintiff brought a post-trial motion seeking to overturn the decision, and the court ordered a new trial.

Background: In September 2009, a 44-year-old man suffered a shoulder injury and was prescribed pain medication by his primary care physician. Following complications from the medication, the patient was prescribed Suboxone to treat an opioid addiction on a monthly basis for approximately three years. According to Centers for Disease Control and Prevention (CDC) guidelines, a pneumococcal vaccine is recommended for patients with a history of substance abuse. Although the patient's medical history, treatment, and diagnosis met the risk factors set out by CDC guidelines, his physician did not discuss or advise the patient to receive a pneumococcal vaccine.

In August 2013, the patient experienced chest congestion and difficulty breathing, which he reported to his physician. The physician advised the patient to come in for a scheduled appointment the following day. At approximately 3 a.m., the patient sought emergency medical help and called 911; he was transported to a nearby hospital. At the hospital, the patient presented with symptoms of respiratory distress: his recorded breaths per minute was 40, compared to a normal rate of 15 to 20 per minute; his blood oxygen level was initially 97 and subsequently dropped to 94; and his heart beats per minute was > 140.

After the patient arrived at the hospital, he was placed in a bed and his condition was observed as he gradually worsened until he suffered respiratory arrest, which led to his death. The hospital did not perform an arterial blood gas test. Throughout his hospitalization, the patient was left unattended for 12 minutes, at which time the patient coded and most likely suffered the permanent damage leading to his death.

The patient's surviving spouse brought a medical malpractice action against the hospital, seeking $16 million in damages and alleging that the hospital was liable for the physicians' negligence under a theory of vicarious liability, whereby an employer is responsible for conduct of the employee. According to the plaintiff's expert, when a patient presents with these types of distress signs, performing an arterial blood gas test is appropriate to measure the patient's respiratory status. The defendant hospital denied liability.

After a seven-day trial, the jury deliberated for 14 minutes and found the hospital not guilty. As a result of this expedient deliberation, the plaintiff filed a motion for post-trial relief, arguing that the jury failed to give thoughtful and careful consideration to all the evidence presented. The court granted the plaintiff's motion and ordered an evidentiary hearing and new trial concerning liability and damages, overriding the jury's defense verdict.

What this means to you: In this matter, the plaintiff's expert provided compelling testimony that left little to no doubt as to the fact that if the patient had been placed on a ventilator immediately on arrival to the hospital, the injury leading to his death could have been prevented. The expert opined that the patient most likely suffered the bulk of the anoxic brain injury during a 12-minute period during which he was not supervised by care providers. The patient's chart confirmed that the hospital staff

failed to monitor and record his vitals during this time window, and his condition progressively worsened. If the patient had been intubated prior to coding, hospital staff would have been alerted immediately because the ventilator is equipped with several alarms that sound if even a single breath is missed. According to the patient's expert, emergency department (ED) staff breached the standard of care by acting negligently in multiple ways throughout the patient's hospitalization.

The patient arrived at the hospital in respiratory acidosis likely caused by sepsis from bacterial pneumonia. Although the pneumococcal vaccine most typically is prescribed for patients older than 65 years of age, other circumstances justify its administration. Here, it would have prevented the patient from developing the infection. Arterial blood gases would have indicated that the patient was in critical condition and needed immediate intubation and support for his respiratory efforts by mechanical ventilation. Everything that followed the care provider's failure to rescue this patient was predictable because of the initial deficiencies.

However, another factor may have contributed: The patient had a history of substance abuse. This unfortunate circumstance can be devastating to patients experiencing real life-threatening situations. Many care providers hold a misguided notion that these patients present to EDs not seeking relief from a real disease, but instead seeking narcotics to meet the needs of their addiction. It is an unfortunate circumstance that can complicate care for these patients throughout their lives.

In this instance, the hospital failed to perform an arterial blood gas test upon the patient's arrival, which would have revealed the severity of the patient's condition. Second, despite the patient's chart showing progressively worsening respiratory distress, the hospital staff failed to place the patient on a ventilator, which would have maintained the patient's oxygen levels by mechanically controlling his breathing. Third, staff failed to supervise the patient during a critical period for 12 minutes, which caused them not to notice that the patient had suffered a severe anoxic episode.

What followed the seven-day trial was surprising, as the jury deliberated for only 14 minutes, far shorter than is typical and a patently insufficient amount of time for any meaningful discussion or evaluation of the facts and law. Despite strong evidence showing that the care providers had acted negligently, the jury returned a verdict in favor of the hospital. While the defendant care providers were satisfied, the plaintiff brought a post-trial motion arguing that the jury shirked its responsibilities and did not deliver a verdict after careful and thoughtful consideration.

It remains unclear whether the patient successfully presented sufficient evidence to establish that the defendant hospital was obligated to supervise the ED physicians and, if so, whether such duty was breached. The care providers argued that there was no relationship between the physicians and the hospital and that the hospital had no duty to supervise. Given the unique procedural issues in this case, this issue remains unsettled. But it is unlikely that the hospital will be able to defer all liability to the individual physicians. Most ED physicians are independent practitioners who contract with hospitals but are not hospital employees and not under hospital supervision. Nevertheless, hospitals cannot evade liability by classifying all care providers as independent contractors, particularly because staff and other support personnel are proper employees and their negligence can give rise to malpractice liability.

The trial court agreed in part with the questions concerning the jury's conduct, and ordered an evaluation and hearing concerning the jury's actions and efforts. The trial court also ordered a new trial. Although this case resulted in a mixed determination — initially favorable for the defendant care providers but ultimately uncertain as to the final result — an important lesson can be learned that is applicable broadly to medical malpractice actions. It is critical to evaluate litigation during all stages, from pre-litigation considerations when a patient suffers an unexpected harm and begins to inquire or request records, all the way to post-verdict, as in this case.

A jury's rendering of a verdict is not necessarily the end of a malpractice case because of appeals. Care providers may be put in the opposite position, whereby a jury rules for a patient — when the evidence does not support that ruling or if the jury rushes the decision. Under these circumstances, an evaluation of the facts and procedures to determine the propriety of post-trial challenges and appeals is crucial. Juries make mistakes or can be reckless in their efforts, but this is precisely why the legal system includes checks and balances to remedy such circumstances. Working closely with counsel is important to assess viable challenges, whether those be factual or procedural, with the trial court or to an appellate court. ■

REFERENCE

Decided on Oct. 29, 2020, in the Court of Common Pleas of Luzerne County, Pennsylvania, Case Number 2015-7551.