HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE SINCE 1979

INSIDE

Relias Media

MARCH 2024 Vol. 46, No. 3; p. 25-36

AI Creates Liability Risks for Healthcare Organizations

Artificial intelligence (AI) is entering a variety of industries including healthcare, where it offers the opportunity to improve diagnoses and patient care in many ways. The potential benefits come with significant risks that must be anticipated and mitigated.

More basic forms of AI have been around for a while, and their use was limited, but that is changing rapidly, says **Sue Boisvert**, BSN, MHSA, CPPS, CPHRM, DFASHRM, senior patient safety risk manager with The Doctors Company, a malpractice insurer based in Napa, CA. ChatGPT changed the face of AI by entering many aspects of society quickly.

"It's hard to predict what's going to happen in 2024, but I think what we need to pay attention to in healthcare — and especially risk managers — is that it is very clear that there needs to be some guardrails around the advanced AI," Boisvert says. "The federal and state governments are starting to create some regulations, and we need to be aware of those and start incorporating those models."

> "WHAT WE NEED TO PAY ATTENTION TO IN HEALTHCARE — AND ESPECIALLY RISK MANAGERS — IS THAT IT IS VERY CLEAR THAT THERE NEEDS TO BE SOME GUARDRAILS AROUND THE ADVANCED AI."

The most prominent regulations or guidelines come from the National Institute of Standards and Technology (NIST), Boisvert says, and IT departments in healthcare organizations must be familiar with that framework. It is easy to implement, and it is based on the idea that organizations should map,

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

HEALTHCARE RISK MANAGEMENT™

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

GST Registration Number: R128870672

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

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

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

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

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

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

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

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

measure, and manage their use of AI, she says.

The first crucial step is to know where AI is being used in the organization. "They need to know whether they're chatbots or AI, what healthcare instruments they're using that are augmented by AI," Boisvert explains. "The reason that it's so important for them to be aware is if you're using an instrument on a patient, you need to be aware of the functionality and you need to be aware of the risks to watch out for."

Two things make this a distinct challenge in healthcare, Boisvert says. First, most providers or risk managers never received any education in advanced computing. Second, there is currently no commercial insurance product specifically dedicated to AI.

"When telehealth first came out, a lot of the professional liability companies added a rider or language for telehealth, but we're not seeing that with artificial intelligence," Boisvert says. "I think there are a lot more risks associated with a program that assists in decision-making than there is with videoconferencing software. Organizations will have to give thought to whether their current policies cover it."

AI risk management should begin with the earliest consideration of introducing AI to the clinical process, Boisvert says. She suggests using the NIST framework when purchasing AI, noting that it should be introduced only as an aid to clinicians and not a replacement for their judgment.

"People will tell you that their product is diagnostic. That's kind of a misnomer. The only person who can diagnose is the provider," Boisvert says. "The artificial intelligence can make recommendations, but the diagnosis is up to the physician. If you're going to use an advanced tool to help make a decision, it needs to be fully vetted."

An enterprise risk management approach, looking at the implications in a complex environment, is necessary with AI, Boisvert says. For example, look at how it will affect staff education and training. No physician should use a piece of AI-enabled technology without a good understanding of the capabilities, how it works, what a failure would look like, and what they would do if there was a failure. Support staff need the same understanding.

Every organization should have a multidisciplinary team that guides purchasing, implementation, and use of AI, Boisvert recommends. That team should include end users, administration, finance, and IT. AI purchasing decisions also should be guided by the organizational culture.

"If you're a risk-tolerant organization, your AI implementation is going to look a lot different than that of a risk-averse organization. In fact, a risk-averse organization may be limiting themselves to static algorithms as

EXECUTIVE SUMMARY

Artificial intelligence (AI) is becoming more common in healthcare and offers substantial benefits. There also are serious risks to consider.

- Clinicians may rely too much on AI instead of their own judgment.
- AI may "hallucinate" and offer unfounded assessments.
- The introduction of AI should be carefully controlled.

opposed to generative AI," Boisvert explains. "Organizations need to do their own risk analysis. What's the worst thing that could happen? What would we do about it? Identify the risks, and then they can evaluate whether those risks are present."

If so, those risks must be monitored, Boisvert says. A good method is with scorecards, already common for monitoring many issues in healthcare. "It is really important for IT, leadership, and end users to collaborate on their scorecards because they are known to be so valuable in clinical quality improvement as well as leadership and finance," she says. "They need to apply the same gravitas and dedication to AI monitoring scorecards as they do for their other scorecards."

Not Always Up to Date

One shortcoming of AI might not be obvious to healthcare professionals, notes **Mihai Nadin**, PhD, the Ashbel Smith Professor Emeritus at the University of Texas in Dallas. The technology is not always up to date, and that could have serious consequences in clinical care, he says.

Even with the casual use of ChatGPT, a query about recent events might produce no answer or an incorrect answer because the technology's "learning" stopped a few years ago. Similarly, AI used in healthcare may not reflect the most current thinking or data, Nadin says.

"My major concern is that AI as it is practiced today is generalizing from the medicine of the past, represented by the data that was used in order to train models," he explains. "Generalizing from the past puts us in a really dangerous situation."

The continuing problem of medical errors and iatrogenic harm may be exacerbated by AI that relies on decades of data and clinical assumptions that are now being challenged. "We know for a fact that medical care based on some wrong assumptions is the third most common killer. First is the heart, which means cardiology, then comes cancer and then comes people killed by errors in medical care," Nadin says. "This being the case, the question that should be asked now is if we take advantage of AI, are we going to automate the killing? Are we going to generalize from a model in which medicine, instead of making progress as a discipline on its own, becomes more and more captive to explanations that come from physics and chemistry, and less and less aware of the real complexities of the living of the biological?"

Nadin supports the use of AI to streamline administrative functions and minimize the burden on clinicians. However, he says the use of AI in the actual care of patients should be carefully controlled.

"I'm not very excited by the fact that we're going to automate more and more of what in principle is an activity that involves an interaction between those who provide medical care and those who need medical care," Nadin says. "The automation of anything that has nothing to do with the patient is, for me, not 100% justified. Don't start automating things related to the relationship between the patient and the doctor."

Risk managers should be concerned about whether AI will diagnose accurately and whether a physician is going to overly rely on an AI model to make that decision, says **John F. Howard**, JD, senior attorney with Clark Hill in Scottsdale, AZ.

"There also is concern over whether there is any inherent bias that is built into the training algorithm of the AI, which may impact certain populations based on bias," Howard says. "Then, of course, there is cybersecurity because there are always privacy concerns when you're training these things. We have physicians turning over large amounts of identifiable data to try and train the AI, or we have third-party vendors that just ended up with access to the whole trove of electronic health records. From a risk perspective, there's a large amount of risk in here that up until now is largely unregulated."

Not all AI products in the healthcare setting are the same and have the same sort of risk associated with them, says **Paul F. Schmeltzer**, JD, senior attorney with Clark Hill in Los Angeles. One way to look at AI products is to categorize their risks from unacceptable to minimal or no risk, he suggests.

"Is this going to be a product or service using AI that providers will lean on to their detriment — meaning it will be a disservice to the patient, whether it's a misdiagnosis or incorrectly prescribing medication, based on overreliance on the AI?" Schmeltzer asks. "Or, does it introduce the risk of something even more nefarious, like the discriminatory aspect of what the AI might spew out as a result of its algorithm, with an inherent bias baked into that?"

More Guidance Coming

Healthcare organizations need more guidance on how to introduce and monitor AI, says **Robert Andrews**, JD, CEO of Health Transformation Alliance (HTA) in Washington, DC, which oversees the strategic direction of more than 50

major corporations to fix the U.S. healthcare system.

HTA is set to release suggested ethical practice guidelines for the use of AI and healthcare soon, Andrews says. The guidelines will address the proper balance between humans and AI. As an example, Andrews notes that when AI scans radiology studies, the error rate is only slightly higher than when a human performs the analysis. But when the AI looks at the study and then a skilled, experienced radiologist also checks it, the error rate is much lower.

"That's what we're after," Andrews notes. "We want the right balance of the AI and the human, who has a perhaps more nuanced understanding of what's going on with the patient."

Additionally, the guidance will caution against AI perpetuating prejudicial patterns based on outdated or uninformed learning. The guidelines also will call for "maximum appropriate transparency," according to Andrews.

"It's a little tricky to define, but we do think that when someone's data is being used in a way to feed an AI algorithm, to the extent it's practical, they should know that," he says. "That is not to say that necessarily patients have the right to opt out, but we just think that when someone's personal information is being used in a database, they should know it, and consent to it where appropriate."

Need Sufficient Infrastructure

A hospital or health system incorporating AI must first ensure it has the appropriate cybersecurity in place and the appropriate infrastructure to handle any type of software that employs AI, says **Bill Bower**, senior vice president with Gallagher Bassett, a healthcare professional liability claims and risk management consulting company in Rolling Meadows, IL.

Bower has seen health system C-suites push for the rapid implementation of AI without first considering all the underlying IT support it requires and the security additions it might entail. He advises a slow and deliberate approach to incorporating AI into a healthcare organization.

Bower also is concerned that the use of AI may increase the potential harm from a ransomware attack. "I start to worry that if we use AI and have a robust database, threat vectors will say, 'Not only do we have your system hostage, but we also could contaminate all your data. And by contaminating all your data, we completely ruin the ability to engage in artificial intelligence and machine learning,'" Bower says. "It hasn't happened yet, to my knowledge, but I certainly could see it as a high-stakes game for those institutions that rely on it."

On the plus side, AI could improve patient care in areas like telehealth services, says **Jolie Apicella**, JD, partner with Wiggin and Dana in New York City. There are risks, but healthcare organizations should balance them with the potential benefits.

"There is the possibility of reducing costs and making healthcare more accessible to larger populations. With the advent of the wider use of telehealth, we saw that certain demographics, [such as] indigent people, were having greater health results and greater access to healthcare," Apicella explains. "I

Safety Strategies to Minimize AI Risks in Healthcare

The following patient safety and risk management strategies for AI in healthcare are offered by **Sue Boisvert**, BSN, MHSA, CPPS, CPHRM, DFASHRM, senior patient safety risk manager with The Doctors Company in Napa, CA:

- Review and apply the National Institute of Standards and Technology AI risk management framework (https://bit.ly/42pIkmr) and the HTI-1 final rule to the organization's AI systems (https://bit.ly/3HP7XmR).
- Check current insurance policies and ask the insurance companies about AI-specific products.
- Form a multidisciplinary team to guide AI purchasing, implementation, and use.
- Educate and train staff on the functionality, risk, and performance of AI-enabled instruments.
- Develop and monitor scorecards for AI performance and outcomes.
- Address the issues of billing, documentation, and reading of different portions of the AI-augmented computed tomography angiography scan. ■

would expect the same results with AI if you can just open a computer and start to have an honest dialogue about all of the symptoms because sometimes you have a limited amount of time with your doctor. But I think there needs to be humans involved. Otherwise, the less human oversight there is into this, I think the greater the potential risk."

Subject to Liability

Healthcare systems and providers may be subject to liability for AI systems under a malpractice theory or other negligence theories when using AI tools to provide care to patients, says **A.J. Bahou**, JD, partner with Bradley Arant Boult Cummings in Nashville, TN. Likewise, AI vendors might be subject to product liability regarding the AI tool used in healthcare.

"Regarding doctors, they should be concerned about using a new AI tool because that tool could be criticized as deviating from the standard of care," Bahou says. "Until the AI tool is widely used and accepted by the medical profession, doctors should always evaluate the outputs from AI tools and maintain the physician's judgment in the ultimate decision on patient care. Until AI tools become part of the standard of care by the profession, this early adopter concern will be a persistent risk by the doctor, and vicariously by the health system, during this evolution of using AI tools in healthcare."

There also is a product liability risk for the AI system designer, such as for the design of the algorithm used in the AI tool, Bahou notes. In this instance, the AI vendor could be liable for the product if it causes harm to the patient. Legal theories in this area could include failure to warn about risks, poor design, unmanageable adjustments to the algorithm due to updates in the machine learning process, or manufacturing defects. For example, if a surgical robot is driven by AI algorithms and causes harm, the AI manufacturer might be liable for that injury to patients if the product is proven to be defective, Bahou explains.

AI vendors are promoting AI assistant tools for the physician-patient interaction, Bahou notes. The benefit is like having a smart speaker, such as Alexa or Siri, listen to the physician-patient conversation and transcribe that conversation. The transcription can then become the medical record of that visit. Providers will appreciate the reduced burden of taking notes and documenting everything, Bahou says.

"The doctor may also ask the AI tool for assistance in diagnosis, allergic interactions, medical history, or prescription assistance. In doing so, the AI system can check the patient's medical history, automatically find available time on the patient's mobile device to schedule a follow-up visit, and/or read data from the patient's mobile device for collecting health data as part of the treatment plan," Bahou says. "The AI tool could send the prescription to your pharmacy of choice and automate that e-prescription process. There are many benefits, but also increased risks." Some risks with transcribing the conversation include a concern about how the AI tool will interpret or misinterpret sarcasm, he notes.

There will be more concern about patient privacy, cybersecurity, and inherent bias in AI tools because those methods are implemented more deeply in the spectrum of patient care, Bahou says. Some risks include the risk of malpractice if the provider relies too much on the AI tool for assistance and misses a diagnosis.

"Likewise, the AI vendor may have product liability if its outputs cause harm or fail in meeting the standard of care with an improper diagnosis. Cybersecurity risks remain prevalent but with increasing concern about the biometric data now added to the medical record," Bahou says. "The record of a person's oral conversation being hacked is much more intrusive as compared to a cryptic medical note written by the doctor in the doctor's own words."

Watch for Bias Toward AI

"Technology bias" is a real concern with the increasing use of AI, says **Wendell J. Bartnick**, JD, partner with Reed Smith in Houston. Providers may perceive AI solutions as highly accurate and rely too much on the technology in making treatment decisions rather than use their medical judgment.

Such overreliance on technology could result in negligence lawsuits against providers with allegations that providers did not meet a reasonable standard of care by failing to use medical judgment to override the AI technology's recommendations, Bartnick says. "However, the flip side will likely become true, with claims that providers must use AI technology to meet the prevailing standard of care. A failure to do so may result in negligence claims," he says. "Organizations will need to continue to monitor the quality and use of AI technology when providing patient care."

Providers should update governance and compliance programs to account for the use of AI and other

advanced technologies so that they are appropriately used, Bartnick notes. Organizations should be clear about which technologies may or must be used and when.

Bartnick says there should be a process of approving and introducing the use of AI in clinical care. Healthcare organizations that do not follow an approval process for adopting AI technology in clinical care likely are taking on significant risk.

Many healthcare organizations are creating or expanding existing governance teams and programs to account for the adoption and use of AI technology, Bartnick notes. AI technology proposals should be submitted to the governance team and undergo a formal approval process. Many AI risk management frameworks recommend that AI governance programs be reviewed and approved by the board or other senior management, he says. Corporate compliance/audit teams also should play a significant role in ensuring ongoing compliance with corporate AI policies on adoption and use.

"Many organizations are in the process of improving their knowledge and awareness of AI technology capabilities and use cases, and they are developing governance and compliance processes to account for AI technology," Bartnick says. "While organizations have made significant progress in a short time, significant work remains."

Possible HIPAA Risk

For covered entities under HIPAA, an AI risk arises under Section 1557 of the Patient Protection and Affordable Care Act, says **Bradley Merrill Thompson**, JD, an attorney with Epstein Becker Green in Washington, DC. The Office for Civil Rights (OCR) has proposed a regulation to prohibit discrimination by an algorithm used in clinical care, he says. For developers, the primary risk is a violation of the Federal Food Drug & Cosmetic Act, which regulates medical devices. *(More information is available at: https://www.hhs.gov/civil-rights/for-individuals/section-1557/index.html.)*

"An algorithm can constitute a medical device if it's used in the diagnosis or treatment of a disease or other condition. So much clinical decision support software that provides patient-specific assessments and treatment recommendations qualifies if it isn't exempted," Thompson explains. "Under a 2016 amendment in the 21st Century Cures Act, clinical decision support can be exempt if the basis for recommendation is fully transparent. But that's a difficult standard to meet for a machine learning algorithm."

The primary issue under both laws is whether a clinical algorithm provides variable levels of accuracy depending on the patient demographic or other factors, Thompson explains. An algorithm that is 99% accurate for white males but only 70% accurate for Black females would trigger a violation, he says, but such disparities in performance are common.

The problem for developers is that such variation often is unintentional — it is simply a reflection of the fact that they had less data for one demographic on which to train their algorithm, Thompson says. An algorithm might be undertrained for one minority just because of a lack of data. Both OCR and the Food and Drug Administration (FDA) have wide enforcement powers, he notes.

There are three primary tactics to mitigate the risks related to AI, Thompson notes. The first is to put a governance process in place to ensure that employees use good data management practices to catch the variability before the algorithm is released, Second, testing and auditing the algorithm before it is released is necessary to catch unintended bias.

Finally, healthcare organizations need to put monitoring processes in place because the reliability of these algorithms tends to evolve, and performance for one subpopulation can decline again without anyone intending it, Thompson says.

Must Protect Data

These products, if they meet the definition of a medical device, must undergo the FDA approval process. The FDA legal standard for when the approval process is triggered is an appropriate judgment about when the algorithm can affect the safety or effectiveness of the technology, Thompson says.

"With the rapid rise of generative AI, a whole bunch of people are now focused on figuring out how AI tools can advance healthcare clinically. Many people are calling for federal regulation, not realizing that federal regulation already exists. Many people in this space do not understand the FDA requirements, and don't understand the HHS [Department of Health and Human Services] proposed regulation that will frankly just codify what the statute already requires," Thompson says. "The statute already imposes nondiscrimination requirements, and the regulation will just make it clear how they apply to algorithms. This domain is full of doctors and computer scientists who are not well-versed in the regulatory requirements."

AI tools often need access to lots of data, notes **Melissa Soliz**, JD, an attorney with Coppersmith Brockelman in Phoenix. Healthcare organizations that are interested in using AI tools will need to carefully consider whether they can use those tools in compliance with privacy and security laws.

For example, will the AI developer agree to enter into a HIPAA business associate agreement that will strictly regulate how the AI developer uses and discloses the data? Consider whether the AI tool will run on the healthcare organization's servers or if copies of the data will be hosted, stored, and processed on the AI developer's systems, Soliz advises. Will the AI developer agree to not use the individually identifiable health information for its own purposes to develop new commercial products? Also, does that AI developer have adequate security measures in place to meet the requirements of the HIPAA Security Rule?

"Additionally, AI is not perfect. Every AI product has limitations. Overreliance on AI may expose a healthcare organization to liability for medical errors and misdiagnoses," Soliz warns. "For example, 'hallucinations' are a well-known generative AI limitation where the AI presents a seemingly reasonable response that is factually inaccurate, misleading, or completely invented — even citing fake sources. A healthcare provider using generative AI to create patient notes, a treatment plan, or discharge instructions, for example, should beware of hallucinations and review the AI's response to avoid inaccurate records, medical error or malpractice, and vicarious liability for the healthcare organization." ■

SOURCES

- **Robert Andrews**, JD, CEO, Health Transformation Alliance, Washington, DC. Phone: (847) 273-3880.
- **Jolie Apicella**, JD, Partner, Wiggin and Dana, New York City. Phone: (212) 551-2844. Email: japicella@wiggin.com.
- **A.J. Bahou**, JD, Partner, Bradley Arant Boult Cummings, Nashville, TN. Phone: (615) 252-2242. Email: ajbahou@bradley.com.
- **Wendell J. Bartnick**, JD, Partner, Reed Smith, Houston. Phone: (713) 469-3838. Email: wbartnick@reedsmith.com.
- **Sue Boisvert**, BSN, MHSA, CPPS, CPHRM, DFASHRM, Senior Patient Safety Risk Manager, The Doctors Company, Napa, CA. Phone: (800) 421-2368.
- **Bill Bower**, Senior Vice President, Gallagher Bassett, Rolling Meadows, IL. Phone: (630) 773-3800.
- **John F. Howard**, JD, Senior Attorney, Clark Hill, Scottsdale, AZ. Phone: (480) 684-1133. Email: jfhoward@clarkhill.com.
- **Mihai Nadin**, PhD, Ashbel Smith Professor Emeritus, University of Texas, Dallas. Phone: (972) 883-2111.
- **Paul F. Schmeltzer**, JD, Clark Hill, Los Angeles. Phone: (213) 417-5163. Email: pschmeltzer@clarkhill.com.
- **Melissa Soliz**, JD, Coppersmith Brockelman, Pheonix. Phone: (602) 381-5484. Email: msoliz@cblawyers.com.
- **Bradley Merrill Thompson**, JD, Epstein Becker Green, Washington, DC. Phone: (202) 861-1817. Email: bthompson@ebglaw.com.

Watch for 'Hallucinations' When Using AI for Healthcare

Artificial intelligence (AI) developers caution that there are limitations to the technology. Healthcare organizations must consider them when seeking the benefits AI offers.

AI can be helpful, but it can introduce errors to the healthcare process, says **Tony Lee**, JD, chief technology officer with Hyperscience, an AI company in New York City.

"Proponents of AI in healthcare have long discussed the benefits of leveraging this technology for efficiency and time savings, but there are considerable risks that must be taken into account when developing models for this purpose," Lee says. "One example is the potential risk of hallucinations by large language models when the model misinterprets massive amounts of data. When dealing with an industry that literally makes a difference between life and death, inaccurate outputs from AI models are simply not acceptable. Patients rely on physicians to make quick, accurate decisions when treating illnesses, making human involvement critical throughout the process."

Lee notes one instance in which an oncology nurse was alerted by AI that a patient had sepsis but was confident the diagnosis was incorrect. However, hospital procedure required her to draw blood from the patient due to AI's diagnosis, which could have exposed him to infection.

"In fact, the patient was not septic, which is why it's so important for organizations to remember that humans must always have the final say," Lee stresses.

Although these risks are concerning, Lee says it is important to remember that humans play a role in overseeing AI models and can unlock huge benefits for the healthcare industry. The federal government should consider standard ethical principles for every healthcare AI use case, but in the absence of such legislation, healthcare organizations can take it upon themselves to minimize these risks and potential consequences, he says.

One way to do so is building an ethical AI committee that governs how the organization uses AI, Lee suggests. The most important standard is oversight of AI systems that always puts a human at the forefront of supervising system outputs, he says. Additional considerations include data privacy, mitigating bias, and ensuring the algorithm is transparent. In addition to improving the overall quality of the model's outputs, Lee says these practices will build trust with a public that is concerned with how their data are used by healthcare organizations.

"All organizations need to self-regulate and promote safe use of AI models, but healthcare companies in particular must be stringent in their safety considerations, especially given how much is at stake," Lee says. "An inherent risk with learning models is if there are biases in the training data — especially as it relates to underrepresented population groups. Some examples include race, nationality, and socioeconomic background. Training data transparency and explainability will be critical to build confidence that the model is taking into consideration the many variables that go into patient care."

In addition to benefits and risks in clinical care, hackers can use AI to bolster their threats to healthcare organizations. The next year will have a more challenging digital threat landscape with the rise of AI-driven cyber threats, says **Kevin Heineman**, vice president of corporate IT at Lyric, an AI healthcare technology company in Sunnyvale, CA. The sophistication of these threats, leveraging AI, will transform traditional cybersecurity strategies, necessitating a shift toward more dynamic and comprehensive security measures, he says.

The collaboration between chief information security officers, IT security professionals, and business units in securing AI business processes will be more critical than ever, Heineman notes. This will involve creating AI systems with inherent security features and moving beyond restrictive policies to embrace inclusive, proactive security plans that can adapt to the evolving digital threat landscape.

"In response to these challenges, healthcare organizations should focus on enhancing their cybersecurity infrastructure, investing in advanced threat detection and response systems. Training employees in cybersecurity best practices and the implications of AI in digital security will also be essential," Heineman explains. "As we navigate through the year, a proactive, informed approach to cybersecurity, especially in AI-related areas, will be crucial for safeguarding digital assets and maintaining trust in technology-led processes."

While healthcare organizations must embrace new and emerging technologies, diligence in the selection process is equally important, says **Vince Cole**, CEO of Ontellus,

a records retrieval company in Houston. Adopting AI technologies offers numerous advantages, including enhancing patient care, engagement, operational efficiencies, and clinical advancements, he says, but organizations also must address the ever-changing legal and regulatory landscape, ensure data security, and address ethical concerns.

Continuous monitoring of new technologies is essential for innovation in the healthcare ecosystem, Cole says. Although AI presents opportunities for increased innovation, caution is advised in implementing it in areas where technologies may not be fully developed.

Organizations should view AI as a tool that complements their clients and staff rather than a replacement, Cole notes. While AI can significantly enhance efficiencies and reduce costs, it remains crucial to involve humans in analysis and review to ensure accuracy and quality controls.

"It is imperative for healthcare organizations to integrate these new technologies with a comprehensive oversight plan, enabling continuous monitoring and adjustments to processes, as necessary," Cole says. "This approach will enhance security measures and ensure compliance with regulations."

Cole says AI technologies hold immense potential in the legal and healthcare sectors. This potential lies in the seamless integration of health systems with patient medical and billing records, as well as in the ability of legal industries to access optimal evidentiary materials for their cases.

"However, the healthcare industry has been slow in adopting new technologies, creating a challenging environment for legal entities to navigate the legal system efficiently," Cole says. "Despite this, ongoing back office innovations have already had a significant impact on the storage and sharing of patient data. These innovations empower legal firms to obtain and thoroughly review crucial information, ultimately enhancing the outcomes of their cases for clients." ■

SOURCES

- Vince Cole, CEO, Ontellus, Houston. Phone: (800) 467-9181.
- Kevin Heineman, Vice President of Corporate IT, Lyric, Sunnyvale, CA.
- Tony Lee, JD, Chief Technology Officer, Hyperscience, New York City. Phone: (646) 767-6210.

Daily Safety Call Improves Care at Hospital

A Maryland hospital found that a highly structured daily safety conference call with key clinicians and administrators can significantly improve patient safety.

For the past year, Luminis Health Anne Arundel Medical Center has conducted a daily safety call Monday through Friday at 9:30 a.m., with 60 clinical leaders and administrators invited. The call usually lasts about 25 minutes and has a strict limit of 30 minutes, explains **Christine Frost**, RN, MSN/MBA, NEA-BC, chief nursing officer and vice president.

Frost typically runs the call and uses a structured conversation format to make it efficient and productive. The group usually discusses a couple of ongoing topics, and then some attendees make presentations on other issues. After that, the meeting is opened to allow recognition of achievements, milestones, and other noteworthy announcements from different units.

"That's a great way to kind of kick off the day because we're constantly running around and it just sort of puts a positive spin on that safety call. It also give folks an opportunity to recognize each other and recognize their teams," Frost says. "Then we launch into the safety portion, with me very deliberately asking if there are any current safety concerns, anything overnight that occurred that you would need to report out in this forum. We hear about safety concerns across the entire organization — anything related to staff safety or patient safety."

The representative leaders from those departments can acknowledge the issue, take accountability, and then follow up when the issue is resolved, Frost says. Sometimes, that happens quickly, and a resolution

EXECUTIVE SUMMARY

A Maryland hospital is reporting success with a daily safety call. Attendees report safety issues, receive updates, and can act quickly on concerns.

- The call is limited to 30 minutes.
- Some issues are resolved during the call or soon after.
- A wide range of hospital leaders attend the call.

can be provided while still on the call. Or, someone can tell the representative that they will call them directly after the meeting to discuss the problem, or that someone is on the way immediately to address it. Other updates or resolutions are emailed or announced on a following call.

"It's really neat that people can say, 'I know every day I'm going to hop on a safety call at 9:30 and I can report things and have an expectation that an accountable party is going to is going to address that safety concern for me as an employee,'" Frost says.

The last topic for the call is the daily update on capacity, leading to any staffing concerns, which links closely with safety, Frost says. Once a week, the call includes an update from infection prevention on hospitalizations and trends.

"It is a very collaborative, very robust discussion. The president of the organization closes this out at the end and usually also recognizes the effort and the team," Frost says. "It really is a forum where we have learned to be very transparent, raising safety concerns, and also creating that closed-loop communication so that we are aware when things are resolved, or what the action plan is to get them resolved."

Attendees include clinical directors who oversee specific areas, local unit leaders, system roles, and key administrators. A representative from the hospital's patient family advisors program attends.

"Probably once every couple of months, I get an email from that patient's family advisor making recommendations about how the call is managed and then also recommendations around something that was reported. I think that's just a really great demonstration of how intentional we are and how much our culture is focused on creating open lines of communication," Frost says. "Here's a community member who is functioning as a patient family advisor and feels comfortable reaching out to me electronically to say, 'I think that maybe we could look at this differently.' That's exactly why we include them in all of the work that we do."

Rounds and Huddles

The work does not end when the daily safety call is complete. Three times a week, purposeful safety rounds are booked from 10 a.m. to 11 a.m. The rounds include the president, Frost, the chief medical officer, the chief operating officer, and additional leaders across the organization. They visit at least two — and usually three — departments.

"We go to where the work is happening and we provide a summary of what was reported on safety calls, a summary of any employee injuries so that we are having conversations with our employees about how to stay safe in the workplace," Frost says. "We also ask them to report any safety concerns that they are experiencing in their workplace. Our intent there is really to be visible, accessible, have open lines of communication,

Speedy Response to Concern During Daily Safety Call

The daily safety call at Luminis Health Anne Arundel Medical Center in Annapolis, MD, often identifies issues that need attention. Some problems take a while to address, but others can be resolved quickly.

Christine Frost, RN, MSN/MBA, NEA-BC, chief nursing officer and vice president, offers this example:

The hospital had been undergoing construction in the main lobby area where most community members arrive and where staff enter for their shifts. There have been many planning meetings with the facilities team, safety and security, and the construction company about how to minimize disruption. Hospital leaders thought they had checked all the boxes.

Once the construction phase began, it became apparent that a few things had been overlooked. In a daily safety call, attendees expressed concern that both visitors and staff were struggling to understand how to safely enter and exit the building.

"We were able to quickly change the signage and change some of the elements around the construction in order to make sure that people could easily access the building. If we had waited for a committee meeting, it would have taken some time," Frost explains. "But because it was raised in that moment, somebody said they would go out immediately after the safety call and add some additional signage so that it's less confusing for our employees and less confusing for patients and visitors coming into the building. That's a rapid response." ■

and then also empower the staff to problem solve when it's appropriate."

Luminis also has shift change huddles every morning and evening, plus a twice-daily bed board to address capacity and staffing. The unit-level huddles are typically attended by everyone on the outgoing and incoming teams. They usually last about three to five minutes and follow the same basic format as the daily safety calls.

"They're a little bit more rapid-fire because folks are trying to hand off and either leave for the day or get their day started," Frost says. "But the goal is the same as with our daily safety call. We want to share information that will help us improve patient safety, employee safety, and quality of care." ■

SOURCE

- **Christine Frost**, RN, MSN/MBA, NEA-BC, Chief Nursing Officer and Vice President, Luminis Health Anne Arundel Medical Center, Annapolis, MD. Phone: (443) 481-1000.

Uptick in Surgical Fires Prompts Concern, Requires Action

A recent report on operating room (OR) fire safety warns that the risk of flash fires is a growing concern as hospitals see more use of high-tech and high-temperature devices in oxygen-rich settings.

Approximately 650 OR fire events are reported in the United States each year, according to the report from Chubb, an insurance company in New York City. In addition to the physical risk to patients and clinicians, organizations can face reputational damage and significant liability exposure, the report authors noted.

Chubb cited one recent study of 139 lawsuits involving operative burns and surgical fires that revealed 60 of the incidents resulted in a plaintiff settlement or verdict, with damage awards as high as $518,000 and a median payout of $215,000.

"With the current litigation environment returning 'nuclear' verdicts aided by social inflation, damage awards have the potential to increase substantially," the report authors cautioned. They noted that The Joint Commission requires accredited organizations to report OR fires under its Sentinel Event policy. *(The report is available online at: https://bit.ly/42ujZvO.)*

The insurer began investigating OR fires and creating the report as a helpful resource after seeing an uptick in OR fire reports in the last two years, says **Diane Doherty**, MS, CPHRM, senior vice president for the Healthcare Industry Practice at Chubb.

"We hope that risk managers take these resources that we have and bring it back to their organization, their safety committees, and say, 'We're starting to see an uptick. What else can we do? Are we making sure that we recommit ourselves to surgical fire prevention, conduct, maybe a pre-risk assessment, and those response protocols?'" Doherty says. "'Are we always up to date as we can be with new technologies with new antiseptic solutions? Are we making sure we have everything that we need to prevent a fire?'"

A key goal is ensuring staff understand the risks of fire in the OR and how it happens, says **Caroline Clouser**, CPCU, executive vice president for the Healthcare Industry Practice at Chubb.

"We have to remind them that there are ignition sources in the operating room and things that can ignite that very easily. Nothing has changed in the surgical procedures drastically to add that exposure. There have been some small changes, like the increased use of cauterization," Clouser says "It's about making sure that, yes, the heat element is important, the other products are important, but it's putting them together that creates fire." ■

SOURCES

- **Caroline Clouser**, CPCU, Executive Vice President, Healthcare Industry Practice, Chubb, New York City. Phone: (212) 827-4400.
- **Diane Doherty**, MS, CPHRM, Senior Vice President, Healthcare Industry Practice, Chubb, New York City. Phone: (212) 703-7120. Email: diane.doherty@chubb.com.

COMING IN FUTURE MONTHS

- HHS proposes cybersecurity requirements
- Trends in medical malpractice claims
- How to handle patient and family complaints
- Latest cyberthreats to healthcare

HEALTHCARE RISK MANAGEMENT™

CME/CE INSTRUCTIONS

To earn credit for this activity, please follow these instructions:

1. Read and study the activity, using the provided references for further research.

2. Log onto **ReliasMedia.com** and click on My Account. First-time users must register on the site. Tests are taken after each issue.

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

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

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

CME/CE QUESTIONS

1. **What does Sue Boisvert, BSN, MHSA, CPPS, CPHRM, DFASHRM, say is the crucial first step in artificial intelligence (AI) risk mitigation?**

   a. Know where AI is used in the organization.
   b. Obtain insurance that will cover AI-related claims.
   c. Restrict the use of AI to highly complex clinical cases.
   d. Allow AI only for administrative purposes.

2. **How could using AI make a healthcare organization more vulnerable to hackers?**

   a. Threat vectors could hold the system hostage and contaminate data.
   b. Threat vectors will impersonate the organization's AI system.
   c. Threat vectors will slow the response of an AI system.
   d. Threat vectors could infiltrate the AI system long before any breach is discovered.

3. **What is the strict time limit for the daily safety call at Luminis Health Anne Arundel Medical Center?**

   a. 15 minutes
   b. 30 minutes
   c. 45 minutes
   d. 60 minutes

4. **What does Caroline Clouser, CPCU, say is a key goal in minimizing operating room (OR) fires?**

   a. Avoiding cauterization.
   b. Ensuring staff understand the risks of fire in the OR and how it happens.
   c. Limiting the use of flammable gases.
   d. Moistening drapes and other flammable material.

CME/CE OBJECTIVES

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

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

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

Mixed Defense Rulings Related to Patient's Death Yield Lessons Regarding Experts

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

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

News: A man underwent spinal surgery and noticed substantial drainage at the surgical site shortly thereafter. Despite multiple follow-up visits to the physician and the physician's practice group, the drainage continued, and the patient's condition worsened. The physician prescribed antibiotics and otherwise told the patient to lie flat and wait. The patient eventually died from an infection.

The patient's surviving spouse filed a malpractice and wrongful death action, alleging that the failure to timely diagnose and treat the patient was malpractice. The patient's surviving spouse named the defendant physician, the medical practice group, and the surgery center. The defendants denied liability. The trial court granted a defense motion, dismissing all defendants, which was appealed. The appellate court confirmed dismissal for the practice group and surgery center but reinstated litigation against the physician. The varied results offer lessons in using and handling experts.

THE APPELLATE COURT CONFIRMED DISMISSAL FOR THE PRACTICE GROUP AND SURGERY CENTER BUT REINSTATED LITIGATION AGAINST THE PHYSICIAN.

Background: On Feb. 19, 2015, a man underwent spinal surgery, a decompressive lumbar laminectomy on the left L4-5 with discectomy. The surgeon informed the patient and his wife that the surgery had gone well, except that something had been "nicked." The surgeon informed the patient's wife that the patient should lie flat on his back for a few days.

On Feb. 25, the patient noticed drainage from the surgical site and that his clothing in the back was soaked. The patient informed the surgeon that day, and the surgeon told the patient to go home and lie down because it would take time.

On March 3, the patient's wife again contacted the surgeon requesting an appointment because the patient's drainage had worsened. The patient and his wife returned to the surgeon's office that day and saw a registered nurse practitioner who noted that the patient reported clear drainage from the incision and a positional headache. The nurse practitioner likewise informed the patient to return home and lie down but to come back the following day if it was still leaking.

On March 4, the patient's incision continued leaking. The patient and his wife returned to the surgeon's office. The surgeon suspected that the patient was experiencing a cerebrospinal fluid (CSF) leak. The surgeon told the patient to get bed rest until his suture removal appointment on March 9.

However, when the patient returned on March 9, the surgeon determined that the sutures should not be removed given the continued drainage. The surgeon prescribed antibiotics and sent the patient home. Two days later, the patient noticed yellow pus coming from the wound. When the patient returned to the practice, he had a temperature of 99.4 degrees and reported intermittent chills, more yellow drainage, and lower back pain around

the incision. A nurse visited the patient's home over the following weekend to perform wet-to-dry dressing changes.

When the patient returned the following Monday, the nurse reported that the wound had significantly worsened, and the patient was admitted to a nearby hospital. On March 20, the surgeon performed a second surgery to fix the leak in the spinal area. However, the surgeon did not find a leak, and a culture of the wound did not show signs of infection. The patient's condition continued to worsen, and he died on April 10, 2015. The patient's discharge summary from the hospitalist noted suspected meningitis and suspected septicemia.

The patient's spouse filed a medical malpractice and wrongful death action against the defendant care providers, including the surgeon, his practice, and the medical center. The plaintiff alleged that the surgeon breached the applicable standard of care by failing to timely diagnose and treat the patient, particularly given the drainage. The defendants denied liability.

On Sept. 14, 2021, the litigation proceeded to a jury trial. The plaintiff presented testimony from two experts, including an orthopedic surgeon with experience in treating patients with postoperative lumbar wounds, and an infectious disease expert. The expert surgeon testified that a dural tear occurred during the first surgery, but that the defendant surgeon was not at fault because such tears can happen to anyone. The expert further noted that once the leak was known, more should have been done, and the patient's life could have been saved by earlier diagnosis and treatment. Similarly, the infectious disease expert testified that the patient had an unresolved infection from the initial surgery, and earlier diagnosis and treatment would have prevented the patient's death.

The trial court granted the defendants' motion for a nonsuit, and the plaintiff appealed. The appellate court agreed in part: It affirmed a judgment dismissing claims against the defendant medical practice and defendant surgery center, but it reversed the dismissal as to the defendant surgeon. The appellate court noted that the plaintiff's experts held differing opinions about what fluid was leaking from the patient's incision, but that did not invalidate their opinions.

What this means to you: In this case, there were multiple forms of malpractice as alleged against the various care provider defendants. The allegation against the surgeon was that his failure to timely diagnose and treat the patient constituted malpractice. Factually, there was no dispute about the patient's cause of death — it resulted from an infection. Legally, the defendant physician's initial challenge to the plaintiff's case was not to directly attack that factual premise itself, but to instead challenge the plaintiff's experts. The defendant physician claimed that the two experts' disagreement was so contradictory and conflicting that it provided no basis for the jury to determine malpractice. Although this was initially successful, the appellate court reversed that determination.

The appellate court recognized the experts' disagreement but noted that the disagreement pertained to the nature of the fluid leaking from the patient's surgical site and the origin of the infection. Although the experts were retained by the same side — the patient's surviving spouse — the experts did not agree on these two items. This provided the defendant physician an opportunity to note that discrepancy within the same party's side and to claim the inherent contradiction and conflict barred recovery. The appellate court looked to the basis of the disagreement and found that whatever the fluid was, and whatever the origin of the infection was, it was not disputed that fluid was draining and an infection occurred.

Typically, experts are a vital resource in medical malpractice cases for both sides, which leaves opportunities for defendant care providers to evaluate an opposing side's experts. Experts can be directly attacked based on a lack of qualifications or a lack of specific expertise, particularly when a specialized area of medical practice is involved. Alternatively, as in this case, an expert's opinions can be the basis for challenge, whether those opinions fail to stand on their own or whether those opinions conflict with other issues in the matter. As recognized by this appellate court, a difference of opinion is not inherently fatal, even if the experts represent the same side.

Nevertheless, to the extent possible, it is beneficial for one's experts to maintain consistency. If a medical provider retains and proffers the opinions of multiple experts, they should consider consulting each other before reaching conclusions, or the provider could independently evaluate the expert's opinions before offering that individual as an expert to prevent contradictory opinions. In this case, the plaintiff's experts did agree on the core issue of the physician's failure to diagnose and treat the infection. Both opined the defendant physician should have taken further steps to diagnose and treat the patient's infection. The appellate court noted that resolution of these issues was proper for the jury and that the trial court ignored evidence and usurped the jury's role.

The allegations against the medical practice and surgery center were based on a claim that the registered nurse practitioner violated the standard of care by not contacting her supervising physician. The trial court recognized, and the appellate court affirmed, that the uncontradicted evidence showed the nurse did contact her supervising physician. She spoke with the physician before she wrote the March 13, 2015, orders. Both the nurse and the supervising physician testified to that fact.

In addition to the issues with the expert witnesses, the fact that the patient's frequent cries for help were not immediately addressed is troublesome. A basic premise in risk assessment is that when the expected outcome varies from what is usually experienced by other patients with similar diagnoses and the patients return or call continually, there is a problem. To assume that this patient is just not tolerating postoperative pain or mobility restrictions is dangerous. Spinal fluid leak is a possible problem after any spinal surgery, especially with a dural tear. The fluid could have been tested to confirm its existence. However, the fact that the patient was experiencing headaches, a common side effect of a CSF leak, should have made the leak known to all practitioners. In addition, a leak of any fluid from a sterile area of the body is a passageway for infectious bacteria. These are not uncommon findings for this type of procedure, but they are externally dangerous when ignored for any significant amount of time. ■

REFERENCE

- Decided Jan. 8, 2024, in the Superior Court of Pennsylvania, Case Number 368 MDA 2022.

Defense Decision Reinstated for Patient's Failure to Provide Expert Testimony

News: A man suffering from complex regional pain syndrome (CRPS) in his ankle underwent surgery, but the procedure was complicated by a broken drill bit. The patient was informed about the potential for additional surgery and the need for X-rays. When the patient went for X-rays, hospital staff hit his ankle against a desk. X-rays revealed a dislodged surgical screw.

The patient sued the hospital for the dislodged surgical screw, claiming that the staff "ramming" his ankle into the desk caused the dislodging. The patient failed to present an expert to support his claim, and the defendants filed a motion for summary judgment. The motion was granted, then reversed, then reinstated upon multiple appeals.

Background: In May 2015, a man was diagnosed with CPRS in his left ankle. On Dec. 14, 2015, the patient underwent surgery to create an osteotomy, which was aligned and fixed with two screws. However, the surgery did not go as planned: The drill bit broke as the surgeon was drilling a hole in the bone for one of the screws, and shards scattered in the ankle. There was insufficient bone to create a hole for the second screw, but one screw was placed, and the physician hoped that would be sufficient. Following the surgery, the patient was informed about the possibility of additional surgery. No X-rays were taken that day, although the physician informed the patient that X-rays were needed to confirm alignment.

On Dec. 17, the patient returned for a follow-up visit. The physician examined the patient's ankle but was unable to perform X-rays. The physician informed the patient multiple times that X-rays were needed. The patient was prescribed pain medication, and he went to a hospital for X-rays the following day.

At the hospital, the patient suffered an incident where his extended left ankle contacted a desk. The patient claimed his ankle was "rammed" into the desk, while hospital staff claimed it was a "slight bump." X-rays showed a lateral displacement in the osteotomy — the fracture was not correctly aligned. A second surgery was performed on Dec. 24.

Approximately one year later, the patient filed a lawsuit against the hospital, claiming that the impact of his left ankle with the desk caused the displacement and dislodged the surgical screw placed during the first surgery. During the litigation, the patient identified two experts, including the physician who performed both surgeries and the patient's treating physician before the surgeries. Neither physician was designated to testify on the cause of the patient's injuries. The surgeon referred to the patient's displacement as "hardware failure" and refused to opine on the cause. The treating physician similarly stated he could not testify that the impact caused the patient's hardware shift.

Before trial, the defendant hospital filed a motion for summary judgment, claiming that the patient failed to provide expert testimony

as to causation, a necessary element of his case. The patient opposed and claimed that no such expert testimony was necessary, and he nevertheless identified his prior experts. The trial court agreed with the defendant hospital that expert causation testimony was required, and that the patient failed to provide any such testimony.

The patient appealed, and the appellate court reversed the trial court's decision. The appellate court ruled that the patient's injuries did not require a medical expert because a layperson could determine the cause-and-effect relationship. The defendant hospital appealed that decision to the Supreme Court of Kentucky. The supreme court agreed with the defendant hospital and the trial court, ruling that causation was not within lay knowledge, thus an expert is required. As a result, the patient's failure to provide expert testimony supported the trial court's grant of summary judgment for the defendant hospital.

What this means to you: An important lesson from this case focuses on a critical aspect of medical malpractice cases: causation. Generally, the legal standard is that the care provider's conduct must have been a substantial factor in causing harm such that a reasonable person would consider the conduct to have contributed to the harm. If the conduct is too remote or trivial, it will not be considered a substantial factor. At the same time, conduct does not need to be the only cause of the harm. Different jurisdictions may apply somewhat different standards or describe them differently, but the general application is the same: If the harm would have occurred without the care provider's conduct, then the conduct is not a substantial factor.

Causation provides an opportunity for defendants to explore the basis for the patient's injury. If there are alternative sources, care providers could point to those as the source of the patient's harm. In this case, there were at least two different possibilities for the source of the patient's injury. There was no dispute that the patient was injured — the imaging revealed the displacement of the screw. But what caused the displacement was heavily disputed. The patient claimed that his ankle being "rammed" into a desk by hospital staff was the source, while the defendant hospital pointed to the patient's initial surgery, which likewise indisputably had gone awry.

THIS CASE ALSO SHOWS THE IMPORTANCE OF APPEALS — AND EVEN THE IMPORTANCE OF APPEALING APPELLATE DECISIONS.

Fortunately for the defendant hospital, the patient failed to provide an expert to support his theory of causation. The patient argued that he was not required to provide an expert because the injury was obvious, and the cause required no expertise to determine — lay knowledge was sufficient. The trial court and state supreme court both disagreed and noted that the question of causation in the medical context almost always requires expert testimony. There are rare cases where the injury "speaks for itself" and could only have happened based on wrongful conduct. This was not one such case, as the defendant hospital argued and presented expert testimony supporting its argument that the initial surgery could have caused the displacement.

This case also shows the importance of appeals — and even the importance of appealing appellate decisions. At the trial court level, the court agreed with the defendant and granted summary judgment, dismissing the matter against the hospital. However, the patient appealed, and the intermediate appeals court reversed the decision. As a result, the defendant hospital then appealed that reversal, and the Supreme Court of Kentucky agreed with the first determination, reinstating the hospital's dismissal. This chain of events certainly is not typical, but it does show the multiple steps and appellate options. A defendant who believes that a trial court committed an error, or even that an appellate court committed an error, should consider with counsel the options for initial or further appellate review. Appeals can be a time-consuming and arduous process, but in this case, the defendant hospital's decision to appeal the intermediate appellate review was effective: The hospital was again dismissed from the case, a successful defense decision in the absence of a jury.

Finally, note that the initial issue that started the chain of events involved medical equipment failure. The investigation around that fact might have added to the plaintiff's story. Had the drill bit not broken and the surgeon successfully placed two screws, the patient's ankle would have had more stability, and some or all the liability may have laid with the manufacturer. ■

REFERENCE

- Decided Jan. 18, 2024, in the Supreme Court of Kentucky, Case Number 2022-SC-0302-DG.

First HIPAA Settlement for Ransomware, Fine for Phishing

The Office for Civil Rights (OCR) achieved two firsts recently: a settlement agreement related to a ransomware attack on a business associate and the first fine issued for a phishing attack. Both cases hold lessons for other covered entities.

A medical management company filed a breach report with the Department of Health and Human Services (HHS) stating that approximately 206,695 individuals were affected when their network server was infected with GandCrab ransomware in 2017. The company was unaware of the intrusion until Dec. 24, 2018, when ransomware was used to encrypt their files, HHS reported.

"OCR's investigation found evidence of potential failures by Doctors' Management Services to have in place an analysis to determine the potential risks and vulnerabilities to electronic protected health information across the organization," HHS noted. "Other findings included insufficient monitoring of its health information systems' activity to protect against a cyberattack and a lack of policies and procedures in place to implement the requirements of the HIPAA Security Rule to protect the confidentiality, integrity, and availability of electronic protected health information." The company agreed to pay $100,000 to OCR and to implement a corrective action plan. *(The settlement details are available online at: https://bit.ly/3OoXxhP.)*

HHS noted that in the past four years, there has been a 239% increase in large breaches reported to OCR involving hacking and a 278% increase in ransomware. In 2023, hacking accounted for 77% of the large breaches reported to OCR.

OCR also announced a settlement with a Louisiana medical group to resolve an investigation following a phishing attack in 2021. The breach affected the protected health information (PHI) of nearly 35,000 people. The settlement is the first involving a phishing attack under HIPAA.

The medical group's breach report explained that a hacker used a phishing attack to gain access to an email account that contained electronic PHI (ePHI). OCR's investigation revealed that the medical group failed to conduct a risk analysis as required by HIPAA. It also had no policies or procedures in place to regularly review information system activity to guard against cyberattacks. The medical group agreed to pay $480,000 and to implement a corrective action plan. *(The settlement details are available online at: https://bit.ly/42gYBKd.)*

Victims Still Have Obligations

The ransomware settlement shows that covered entities and business associates cannot depend on sympathy from OCR when a malicious actor instigated the breach, says **Claire O'Brien**, JD, an attorney with Brooks Pierce in Greensboro, NC.

"Being a victim is not an excuse for failure to fulfill your legal obligations. HIPAA-covered entities and business associates have an affirmative obligation to assess and mitigate risks, including the risks of cyberattack, whether it's phishing, ransomware, or hacking," O'Brien explains. "Of course, the type and level of risk and the nature of an appropriate preparation for that risk is going to vary from organization to organization. But security is not a set-it-and-forget-it issue."

Organizations that maintain ePHI have to regularly assess their risk and document those assessments, which will be critical if there is a subsequent investigation by HHS, O'Brien says.

It is important not to assume that the ransomware risk is applicable only to large organizations. "We're seeing it impact smaller organizations, too, so it doesn't happen only to major healthcare systems. Everyone, even small providers, needs to be aware of the risk of cyber threats like ransomware hacking attacks because we're seeing these happen regularly," O'Brien says.

O'Brien suggests asking these questions about ePHI and cybersecurity:

- Does the office destroy ePHI that is no longer in use?
- Is there a backup plan or a process to create retrievable exact copies of ePHI?
- Does the organization use a system to assign each user a unique identifier that can be used to track activity within information systems that contain ePHI?
- Are automatic log-off capabilities in place to ensure unauthorized users cannot access data on unattended workstations?
- Is executive leadership or management involved in risk management and mitigation decisions?
- Are security processes communicated throughout the organization?
- Are there sanctions against workforce members who do not comply with security policies?

The ransomware settlement shows that HHS is starting to act against organizations for security breaches triggered by external bad actors, says **Erin Dunlap**, JD, an attorney with Coppersmith Brockelman in Phoenix. The failure to detect the unauthorized access for more than 20 months likely played a significant part in OCR's decision to pursue enforcement action against the management company in this case, she says.

"OCR clearly expects organizations subject to HIPAA to assess their systems proactively and identify and address vulnerabilities," Dunlap says. "While these cyberattacks can be incredibly sophisticated and we may not know the attacker's next move, a good risk analysis and risk management plan with an ongoing review of system activities are important and necessary steps to reduce the risk to your organization."

In the phishing settlement, the key finding from OCR is that the medical group never conducted a risk analysis on its electronic patient data or implemented procedures to review system activity — both of which are required safeguards under the HIPAA Security Rule, Dunlap explains.

"While those actions may not have prevented the phishing attack — often caused by a workforce member opening emails impersonating a known or trustworthy source — OCR is clearly sending the message that these proactive steps reduce the chance that these types of cyberattacks will be successful," Dunlap says. "They are taking enforcement action against organizations that do not take these steps, even when the breach itself is caused by an external bad actor. In this case, the best defense is a good offense."

Dunlap advises being proactive about security measures, monitoring systems, and educating workforce members on phishing and other common cybersecurity attacks. Employees should know what to look for and how to respond when an email or sender "just doesn't look right," she says. ■

HHS Issues HIPAA Best Practices for Telehealth

The Department of Health and Human Services (HHS) published a resource guide to assist telehealth providers in explaining the privacy and security risks to patients, but the guidance makes clear HIPAA does not require this education. However, the goal is for the resource guide to help providers who would like to discuss potential risks with the patient. The resource is intended as a guide to best practices. HHS suggests telehealth providers explain these issues:

- Explain the remote communication technologies that will be used, including examples of different types of telehealth services.
- Discuss the importance of health information privacy and security. Inform patients about the privacy and security protections built into the remote communication technologies used by the provider.
- Describe the possible risks to the patient's information and how to minimize the risks. Explain that using telehealth can put the security of some information at risk. Cover relevant risks, such as viruses and other malware, and unauthorized disclosure of information. Also, discuss mitigation measures such as anti-malware solutions and the use of headphones during telehealth sessions.

Providers also should inform patients about how the provider will contact them, which can help them avoid potential phishing emails or other scams. *(The HHS best practices are available online at: https://bit.ly/48TOI7a.)*

Telehealth best practices are common sense guidelines that should not conflict with current HIPAA compliance efforts, says **Douglas A. Grimm**, JD, partner with ArentFox Schiff in Washington, DC.

"Some of this is straightforward, which is a good thing because it emphasizes privacy and security measures that are important," Grimm says. "When a patient enters into a conversation with a physician, either their guard may be way up or maybe their guard goes down a little bit, just depending upon perhaps their stress level or the pre-existing relationship with the provider. But ensuring that the provider reiterates the information laid out in the OCR [Office for Civil Rights] guidance kind of level sets."

Providers should follow the guidance, but it shows that OCR has an eye on HIPAA compliance as telehealth technologies continue to grow in sophistication and popularity, Grimm says. "There are going to be more lapses," he says. "Unfortunately, that's just inevitable with the growing volume and implementation of telehealth."

OCR's recommendation to educate the patient on the actual technology and the vendor behind the technology is a good move, Grimm says. Providers should explain who owns the technology and who the patient can contact if they have questions regarding the technology.

"I like to see that emphasis out front. In previous guidance, I don't think that point has been emphasized as clearly as it was in this recent guidance," Grimm says. "The other thing I also looked on approvingly was letting the patient know the schedule of communication. I appreciate the guidance OCR says you should make sure the patient understands how they would be contacted by that vendor and in what time frame. If I got an email from whatever the engine is that powers my Gmail account, my initial instinct would be to simply disregard it."

In some ways, the guidelines mirror the protections that many covered entities have put in place already, says **Amy M. Joseph**, JD, partner with Hooper Lundy & Bookman in Boston. Some states already require that providers engage in these types of disclosures as part of an informed consent for telehealth, she says.

"It's a very helpful user-friendly resource. I think for those who aren't implementing these types of measures, it's a good idea to read as a best practice for consideration," Joseph says. "I also think it's important to know OCR is clear that this is not a specific requirement. There's no mandate."

The guidelines are about consumer protection, so it is important to consider your patient population and how much education they might need, Joseph says. "Some patient populations use telehealth all the time and are very comfortable navigating the internet and mobile app," she says. "Others may benefit from more information to make sure they're clear on the risks that they're taking and what it means to use telehealth."

Joseph advocates for transparency and more information for consumers to understand when they use different platforms and different modalities. She notes that the guidelines include references to remote patient monitoring and educating patients to help protect against phishing attacks or other types of scams. Although not strictly related to HIPAA, Joseph notes that there is some scrutiny from HHS in the remote patient monitoring space regarding phishing or unsolicited contact of beneficiaries.

"I think there's a problem. There's a small group of bad actors who will engage in fraud schemes whenever there's a new modality. We saw it in telehealth, and we're seeing it in remote patient monitoring, but that's a very small segment that is separate from the day-to-day telehealth and remote patient monitoring that we're seeing every day," Joseph says. "Patients are benefiting from improved access to care and more efficient care, but there are some segments out there with fraud schemes. It's good to keep an eye out for remote patient monitoring."

Although not required, it is good practice for providers to explain what telehealth is and the remote communication technology used before the telehealth session, says **Paul F. Schmeltzer**, JD, senior attorney with Clark Hill in Los Angeles.

Patients do not always understand that the terms telemedicine and telehealth are sometimes used interchangeably and that a provider may use a diverse array of remote communication technologies (e.g., a telephone, computer, tablet, or smartphone) to conduct a telehealth session, Schmeltzer says. Patients need to understand that telehealth appointments, whether by phone for an audio-only call or through a videoconferencing app, require the same privacy protections afforded to patients under HIPAA for other types of in-person encounters, he says.

"Patients should also understand that telehealth can encompass patients sending healthcare questions and receiving responses from you using messaging technologies or email, or using remote patient monitoring technologies, such as a device to collect vital signs or a video monitoring system to help you keep track of the patient's health, vital signs, and safety from a remote location," Schmeltzer says.

Practices also should explain to patients the possible risks to the patient's PHI and ways that patients can mitigate those risks.

"These risks include unauthorized access due to unpatched software, accidental disclosures when the patient conducts their telehealth encounter in a public location or somewhere prone to eavesdropping, and possible computer viruses or malware on the patient's computer that could infect the software used for the telehealth encounter," Schmeltzer says. ■

Ransom Demands Decrease and More Companies Refuse to Pay

The number of ransomware victims opting to pay the ransom has fallen to a record low, according to the most recent data from Coveware, a ransomware remediation company in Westport, CT. At the beginning of 2019, 85% of ransomware victims paid a ransom. However, that figure fell to 46% in the middle of 2021 and 29% in the last quarter of 2023.

Coveware attributed the decline to "continued resiliency growth in enterprise environments; companies impacted by ransomware are increasingly able to recover from incidents partially or fully without the use of a decryption tool."

Also, the company noted data-driven reluctance to pay for intangible promises from cybercriminals, such as the promise not to publish/misuse stolen data and the promise to exempt the company from future attacks or harassment. *(The Coveware report is available online at: https://bit.ly/42lAHxe.)*

"The industry continues to get smarter on what can and cannot be reasonably obtained with a ransom payment. This has led to better guidance to victims and fewer payments for intangible assurances," the Coveware report authors noted. "The trend aligned with a relative decline in the size of victims impacted and a reappearance of small-game actors groups who reclaimed some market share after previously dropping in frequency during Q3." ■

When a Privacy Breach Is Not a Breach

Language is important when talking about noncompliance with HIPAA, says **Michelle Garvey Brennfleck**, JD, shareholder with Buchanan Ingersoll & Rooney in Pittsburgh. Not every instance of noncompliance is a breach, she notes.

"If I'm counseling a client healthcare organization regarding a potential HIPAA violation, I might refer to it as an 'issue,' an 'incident,' or 'event.' Even 'incident' sometimes carries with it some weight that we might not want to encourage at the beginning of an investigation," Brennfleck says. "Be very mindful of language — both verbally and especially in writing — that you can't take back. You might establish that an incident or an event was not, in fact, a HIPAA breach, and presented a low probability of compromise of that protected health information [PHI]."

Not every unauthorized use or disclosure of PHI necessitates notification, notes **Jody Erdfarb**, JD, partner with Wiggin and Dana in Stamford, CT. For example, if the information is encrypted and the encryption key is not compromised, that is not considered information that triggers the breach notification rule.

Erdfarb recalls one incident in which a farmer in a neighboring town went to a nearby hospice to return a medical record he found in his field, complete with tractor tire marks. He recognized the name of the facility because his wife had been there. The facility determined that a nurse had put materials on top of her car earlier and some papers had blown away. The farmer assured hospice administrators that he had not looked at any information on the document other than the facility name at the top of the page.

"If that's your situation and you're able to get information from the person reporting the breach that it hasn't been impermissibly disclosed by a person who could retain that information, then that's an exception to the breach notification rule," Erdfarb says. "You have that person sign a statement saying that they didn't retain any of the information, and you don't have to make the disclosures under HIPAA in most circumstances." ■