HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE SINCE 1979

SEPTEMBER 2021 Vol. 43, No. 9; p. 97-108

INSIDE

Impaired healthcare workers threaten safety, but need support . . . 101

Respond promptly to billing audits 103

Ransomware, related threats continue 104

Class action suits possible after cyber breach . . 107

Legal Review & Commentary: No liability for hospital under the Emergency Medical Treatment and Labor Act; proposed expert witnesses correctly disqualified, but proper witness disregarded

HIPAA Regulatory Alert: Court rules no private right of action for HIPAA, but questions remain; requirements for retaining HIPAA records

Relias Media
From Relias

Parents Still Unwilling to Speak Up About Safety Issues

For decades, risk managers have tried to improve safety by encouraging patients and family members to speak up when they are concerned about care or suspect something might be wrong. Some progress has been made, but recent data suggest one group remains reluctant to speak up: the parents of pediatric patients.

The Leapfrog Group recently released its Patient Experience Report, featuring the results of surveys administered to patients by hospitals and ambulatory surgery centers (ASCs) across the country.[1] Using results from the Consumer Assessment of Healthcare Providers and Systems (CAHPS) surveys, the Leapfrog Hospital Survey, Leapfrog ASC Survey, and the Centers for Medicare & Medicaid Services (CMS), the report focuses on the patient experience in adult inpatient hospitals, hospitals that treat pediatric patients, and facilities that provide same-day surgeries.

> "MANY PEDIATRIC PATIENTS CANNOT SPEAK UP FOR THEMSELVES, SO IT IS IMPORTANT THAT THE PARENT OR GUARDIAN DO SO, AND THEY MUST FEEL AS THOUGH THEY'RE EMPOWERED TO."

The data indicate that for children receiving hospital care, a significant portion of parents and guardians do not feel comfortable raising concerns about errors.

The pediatric survey "raises serious concerns about patient safety, with only an average of 62% giving the most favorable response on how well they felt equipped to prevent mistakes by reporting concerns," the authors wrote. "Included within this area are parent perspectives on how well the hospital administers medication, an essential step

Financial Disclosure: Consulting Editor **Arnold Mackles**, MD, MBA, LHRM, discloses that he is an author and advisory board member for The Sullivan Group and that he is owner, stockholder, presenter, author, and consultant for Innovative Healthcare Compliance Group. The relevant financial relationships listed have been mitigated. None of the remaining planners or authors for this educational activity have relevant financial relationships to disclose with ineligible companies whose primary business is producing, marketing, selling, re-selling, or distributing healthcare products used by or on patients.

HEALTHCARE RISK MANAGEMENT™

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

GST Registration Number: R128870672

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

JOINTLY ACCREDITED PROVIDER™
INTERPROFESSIONAL CONTINUING EDUCATION

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

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

1.5 ANCC contact hours will be awarded to participants who meet the criteria for successful completion. California Board of Registered Nursing, Provider CEP#13791.

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

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

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

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

to prevent serious potential harm from medication errors, and whether or not hospitals empower parents and guardians with a welcoming, open environment for patients to report concerns."[1]

A parent "may be better equipped than a medical provider to notice when something is wrong. Feeling prepared to speak up immediately when they observe problems is a critical patient safety indicator, improving the odds of preventing or reducing harm from errors," the authors noted. "Many adult inpatients may not fully understand what they need for the continuation of their care after being discharged from the hospital. Patients do not give high ratings to hospital communications about medications — a critical problem for patient safety, since medication errors are one of the most common dangers patients face in healthcare settings."

ASCs received more positive ratings on this issue than hospital outpatient departments.

Parental Observations Useful

The Leapfrog Group and others in the healthcare community have encouraged people to ensure a relative or companion is present to be the patient's advocate and voice concerns, notes **Erica Mobley**, vice president of administration with The Leapfrog Group. Fortunately for most pediatric patients, at least one parent fills that role.

"Many pediatric patients cannot speak up for themselves, so it is important that the parent or guardian do so, and they must feel as though they're empowered to," Mobley says. "When a child is in a healthcare environment, it can be very stressful and worrisome, but parents should never feel that they have to be careful walking around providers and feel that their opinions shouldn't matter."

Parents and guardians know the child better than any provider, so they often will be the first to pick up on subtle differences in the child's behavior or appearance.

"Even a minor change can be the signal that something more serious could be happening, so parents should never feel that they should hesitate — or that if they do speak up, they won't be listened to," she says. "That really was an alarming finding that parents may not feel comfortable speaking up if they think something is wrong."

Mobley encourages physicians and nurses to clearly state they want the parents to speak up if they have any concerns or questions,

EXECUTIVE SUMMARY

Recent research indicates many parents are unwilling to speak up about safety concerns. Encouraging them to speak up will require a culture of safety.

- 62% of parents in a pediatric care setting were confident about voicing concerns.
- Many patients and parents think healthcare professionals will not consider their concerns.
- Physicians and nurses must respond favorably to encourage more parent participation.

emphasizing they should relate even the smallest issue.

"But, of course, you have to not just tell them that. You have to actually be willing to hear them and respond appropriately when they do speak up," she says. "That is the challenge for some organizations."

Some Do Not Know They Can

It is important to tell patients and parents they can speak up because many do not realize they can, says **Karen Curtiss**, founder of The Care Partner Project in Chicago. When her organization holds presentations on the importance of voicing patient safety concerns and asks attendees for the most important thing they learned, Curtiss says a common response is "I didn't know I could ask questions" during a medical visit or hospital stay.

Even those who feel more comfortable speaking up often do not know what to say or ask, Curtiss says. Disparities in education, fluency in English, and familiarity with the healthcare system all can discourage people from questioning what is happening or reporting concerns.

"There also is a sense of time pressure that inhibits conversation. The patient may want to ask what that vocabulary word means or why treatment is proceeding in this way and not that way, but they don't want to take up more of the physician's time when it is obvious they are pressed for time," Curtiss says.

Patients and caregivers also report they fear they will be seen as a "pest" or "difficult" if they ask too many questions or report their concerns, and that such labeling will result in poor care quality. That is why the response of the physician or nurse is so important to ensuring parents feel comfortable speaking up.

"Our greatest fear is that when people do ask questions, they'll get the eyeroll," Curtiss says. "The eyeroll just shuts people down."

The Care Partner Project offers checklists patients and caregivers can use to help them advocate for patient safety and quality. The checklists are available online at: https://bit.ly/3iA73z8.

Hospital Encourages Voicing Concerns

It is troubling that so many parents are reluctant to voice their concerns, says **Michael Loftus**, MD, chief medical officer at Jersey City (NJ) Medical Center.

In some cases, perceived communication barriers can arise from an expertise or knowledge differential, he says. This is not unique to medicine; it is true across many industries. People believe they will not be heard, or that trained professionals know better, so they do not speak up.

"However, patients, family, and caregivers are a crucial part of the healthcare team because they are often attuned to small changes in a patient that a healthcare provider may not see," Loftus says. "For this reason, it's vital that we create a culture where people feel confident about speaking up and asking questions. Indeed, the next generation of medicine — today's residents and fellows — are focusing more than ever on the importance of team-based care. They are being trained to help patients and families feel more comfortable speaking up and communicating their concerns."

Many hospitals — including Jersey City Medical Center and elsewhere in the RWJBarnabas Health system — are high reliability organizations. This involves creating a culture where everybody — not just patients and families — is encouraged to speak up and escalate their concerns.

"We have been focused on this for several years. The process involves daily safety briefings and training people to use common language both to express concerns and receive feedback. Once everyone embraces this culture, every piece of information is treated as valuable, and the dismissive mentality is minimized," Loftus says. "No one is too low on the proverbial food chain to question someone else, and no one is too high on the food chain to be questioned."

No Eyerolls, Please

But encouraging family members to speak up will not work if they are met with eyerolls and dismissive comments. How can clinicians become more accepting and responsive?

This requires proactive training and communication to clinicians so they understand the vital importance of hearing family member input and how to create an environment in which family members feel heard, Loftus says. This might be as simple as sitting down, asking the family about any concerns, and taking a meaningful pause to make it clear you are willing to hear these concerns.

Loftus and colleagues work closely with the entire clinical team to remind them of the importance of respect and meaningful patient engagement.

"Reassure the family that if they have concerns, you want to hear them. Maybe they won't raise them right then and there, but by

setting that tone, you have created an atmosphere in which, at the right moment, they may be willing to speak up," he says. "It's about creating a culture of respect. Every member of the care team deserves our respect, and eyerolls and dismissive comments are the antithesis of respect."

Measuring progress in this area can be challenging. In addition to data from The Leapfrog Group, Loftus looks to Press Ganey patient experience metrics. Many of the same behaviors that tie into creating a culture of communication and respect are reflected in these surveys.

"Another way we measure success is through actual clinical outcomes. Do patients go home healed and in a better place than when they came through our doors? Was their hospital stay satisfactory, with no mishaps?" he asks. "Open communication leads to safer care and better performance. We review our outcomes and our patient surveys rigorously. We read each and every comment we get from our patients as a team. Our processes are focused on getting as much feedback as possible in real time so that issues can be addressed now, immediately — not later, after the patient is discharged, when it's too late."

Continuous quality improvement is key to addressing issues such as parental reluctance to voice concerns. Jersey City Medical Center has seen enormous improvements in recent years by focusing on safety, patient engagement, and giving patients, families, and caregivers the tools and comfort they need to communicate their concerns.

"It's worth repeating that every patient, or their family members and caregivers, should consider themselves among the best advocates for that patient. They should feel comfortable raising any concern at any time. They should remember that there is always another layer — if they feel that their concern has not reached the right ears, that concern can and must be escalated," Loftus says. "If a patient ever feels that their concern is not being accepted at face value by a clinician, they should know that they have the right to escalate that concern higher and higher in the organization until they feel heard." ■

REFERENCE

1. The Leapfrog Group. What patients think about their hospitals and ambulatory surgery centers: An analysis of patient experience surveys. 2021. https://bit.ly/3irflnq

SOURCES

- **Karen Curtiss**, Founder, The Care Partner Project, Chicago. Phone: (847) 208-6074. Email: karen.curtiss@carepartnerproject.org.
- **Michael Loftus**, MD, Chief Medical Officer, Jersey City (NJ) Medical Center. Phone: (201) 915-2215.
- **Erica Mobley**, Vice President, Administration, The Leapfrog Group, Washington, DC. Phone: (202) 292-6813.

Impaired Healthcare Workers Threaten Safety, But Also Need Support

Impaired healthcare workers (HCWs) can pose a serious threat to patient safety, but they must be handled carefully and with respect to their own health conditions. Risk managers must ensure their organizations are prepared to protect patient safety while also working to help impaired HCWs receive treatment and return to work.

Healthcare organizations always faced the problem of impaired professionals and workers, but the issue is receiving more attention now because of some high-profile cases, says **Rebecca M. Lindstrom**, JD, shareholder with Polsinelli in Chicago.

Lindstrom notes the most publicized case of an impaired physician is Christopher Duntsch, MD, PhD, who practiced medicine in Dallas for two years before becoming the first doctor in the United States to be sentenced to life in prison for his practice of medicine. *(For more on the Duntsch case, see "'Dr. Death' Case Holds Lessons for Risk Managers, Hospitals" in the June 2021* Healthcare Risk Management*, at: https://bit.ly/3xBHZMe.)*

In another recent case, Robert Morris Levy, a former pathologist at Veterans Health Care System of the Ozarks in Fayetteville, AR, was sentenced to 20 years in prison. The hospital suspended him for being impaired at work, which the court found led to faulty diagnoses and three deaths. *(More information is available at: https://bit.ly/2VEu230.)*

"We're becoming more aware of it, and people are feeling more empowered to speak out and report when they have concerns," Lindstrom says. "With the #MeToo movement and everything else going on in the past year or so, people are more confident about speaking up about powerful people like physicians. The trend is more people raise a concern because we're seeing what happens when you don't call people out and you let things go on for too long."

Risk managers should ensure education on impairment at all levels of the organization, starting with what defines impairment, Lindstrom says. For example, an HCW can experience a mental health issue while sober. The education also should include instruction on what to do when someone suspects impairment.

"When it comes to physician impairment, the people who are most likely to spot it are those staff who work with them closely behind the scenes — the nurses, scribes, and technicians. They need to know what to look for and how to report it," Lindstrom explains. "They have to know there will not be any retaliation, that they will be protected if they report their concerns."

Follow Through on Reports

The hospital or health system should be prepared to take all complaints seriously by conducting a prompt investigation, she says. Be proactive and refer the HCW to a wellness committee, a physician health program, or rehabilitation program.

One of the biggest mistakes healthcare organizations make with impaired physicians is to not take reports seriously or to only halfheartedly investigate, Lindstrom says. Each report must be fully investigated, rather than simply asking the physician or nurse if they are impaired and then accepting the denial.

"Don't ever say that's enough and you'll just wait to see if anyone else complains, because surely if the professional really is impaired then someone else will report it, too," Lindstrom says. "The risks are too high."

The authors of a 2008 study found 78.7% of physicians were still licensed and working five years after completing a rehab program, compared with relapse rates of 40% to 60% in standard nonphysician programs.[1]

"When you identify an impaired physician and address the problem

EXECUTIVE SUMMARY

Healthcare organizations must offer a program for responding to impaired healthcare workers. The threat to patient safety is high.

- Educate all levels of the organization about the policies and procedures for impairment.
- Ensure no retaliation occurs for reporting concerns about impairment.
- Be flexible in the options for helping someone overcome impairment with various accommodations and treatments.

quickly, there is a high likelihood they are going to be rehabilitated. Focus on rehabilitation and make sure you have a fair process in place," she says.

The organization must write an impaired physician policy that specifies what happens in case of suspected impairment, Lindstrom says. Specific policies and procedures must be in place, but remember some flexibility is required.

"What works for one might not work for another. Have some flexibility to provide reasonable accommodations, or have people work with a therapist, or go to an inpatient program," Lindstrom says. "Don't try to say, 'This is how we do it with everyone,' because with impairment it can be important to tailor the response and the improvement program to what that particular person needs."

Licensing Boards Offer Best Practices

Best practices for impaired HCWs are clearly established through the professional practices board or licensing board in each state, notes **Rich Jones**, MA, MBA, LCAS, SAP, executive vice president and executive director of Heritage CARES, a confidential online recovery program for people and families struggling with substance use disorders, based in Coppell, TX.

Although there might be small levels of variability, most states hold the same expectations, he says. Mandated clinical treatment is used to stabilize the condition and might include detox, rehab, long-term residential, or intensive outpatient care. American Society of Addiction Medicine (ASAM) placement criteria are used to guide decision-making on this level of care recommendation. A qualified professional, such as a licensed counselor, psychiatrist, or a licensed drug and alcohol specialist, will conduct the ASAM level-of-care assessment.

Following clinical treatment and stabilization, the person will engage in long-term monitoring program, 12-step or other recovery groups, random urine drug screens, and ongoing clinical care as indicated. Law enforcement would initiate additional, case-by-case legal consequences in the event a crime has occurred.

"Note that having a substance use disorder is not a crime. However, doing certain things to support that disorder could be a crime. For example, diverting pills or writing illegal/fake scripts," Jones explains. "The addiction is not a crime. But the behavior associated with the addiction is a crime and could be prosecuted accordingly."

Jones underscores the need for flexibility when responding to impaired physicians.

"Do not fall into an automatic one-size-fits-all response. Some people will require detox and inpatient treatment while others may be able to be stabilized via community-based outpatient care," he notes. "A truly individualized assessment should be conducted. Recovery group requirements should be taken into account for multiple pathways, and all avenues should be explored."

Monitoring Periods Vary

Most human resources (HR) departments issue clear guidelines on how to respond to impairment among HCWs, Jones notes. There are limitations consistent with the Americans with Disabilities Act. For instance, substance use disorder is a disease and treatment and/or monitoring must be offered before termination. The professional practices board provides guardrails and guidelines for HR responses.

Monitoring periods vary from discipline to discipline. Physicians are the most intensely scrutinized and monitored.

"The physician monitoring programs are five years in length and have a stunning history of success, with 90-plus percent compliance and completion," Jones says. "This is because physicians are highly motivated to retain their license. Nursing monitoring may be less intense in terms of length of time and requirements."

Union factors must be considered, Jones notes. The collective bargaining agreement in any given system certainly will play into the response. However, all union contracts must comply with the professional practices board/licensing board expectations.

"Therefore, the union cannot protect the healthcare provider from the monitoring programs or board sanctions," Jones says. ■

REFERENCE

1. McLellan AT, Skipper GS, Campbell M, DuPont RL. Five year outcomes in a cohort study of physicians treated for substance use disorders in the United States. *BMJ* 2008;337:a2038.

SOURCES

- **Rich Jones**, MA, MBA, LCAS, SAP, Executive Vice President, Executive Director, Heritage CARES, Coppell, TX. Phone: (469) 293-3175.
- **Rebecca M. Lindstrom**, JD, Shareholder, Polsinelli, Chicago. Phone: (312) 463-6217. Email: rlindstrom@polsinelli.com.

Billing Records Audits Require Prompt, Thorough Responses

A government billing records audit will make most hospital leaders nervous because of the potential financial — and even criminal — consequences, but understanding the process and best practices can alleviate the stress, says **Christina M. Kuta**, JD, an attorney with Roetzel & Andress in Chicago.

The number of audits has decreased in the past year or so, but Kuta says that probably is due to disruptions caused by the pandemic. She expects them to resume in full force soon.

Medicare and Medicaid audits come in several forms, from a general audit to one specifically designed to find suspected fraud. Investigators also may focus on healthcare organizations in a specific geographic region.

A common mistake is failing to respond promptly and appropriately to the audit notice, Kuta says. No matter what kind of audit is occurring, it always starts with a letter from the government. It is important to ensure there are updated mailing addresses for the organization and that mail sent to those addresses is checked regularly. If CMS sends an audit notice to a PO box that is checked only sporadically, you could lose valuable time before the audit date.

"I've had a number of clients who said they never received audit notices and didn't respond to them, and that was a major issue with Medicare. Medicare was able to prove that they sent the notice through a trackable method, but the healthcare organization did not have an organized way for handling that kind of mail, and the notice fell through the cracks," Kuta says. "You have to have a process so that anything coming from Medicare is opened quickly and appropriately."

The audit notice will request certain documents, often referring to specific patients. The healthcare organization responds with the requested documents, then waits for the decision from CMS. Responding promptly is important, yet many organizations do not.

"I can't tell you how many agencies I've seen who consider the response deadline a suggestion and not a requirement. They don't respond by the 30 days or whatever is specified, or they don't send everything they asked for, or they don't respond at all," she says. "Now you've irritated Medicare — and you never want to do that. You also have not helped your case in trying to show Medicare that you're doing everything correctly, you don't owe them any money, and they should leave you alone."

Failing to respond in full by the deadline always is a big mistake. If the records request is burdensome, you can request more time and CMS usually will grant it. Kuta says CMS has never refused to extend a deadline when she asked on behalf of a client.

CMS will either state that it found no problem during the audit or outline what issues were found and how much money it wants refunded.

"Medicare may suspend your payments during the review in certain circumstances as a way to capture that money in case they want money back after the audit," Kuta says.

Audits from commercial payers usually are less extensive than a government audit, but they follow the same pattern and can be prompted by the same factors. For instance, a payer might notice that a hospital, clinic, or home health agency is billing for a certain code at a much higher rate than local competitors.

Commercial payer audits tend to strike less fear in the hearts of healthcare leaders because, unlike CMS, the third-party payers do not carry the threat of criminal penalties or kicking the organization out of government programs, which would be a death sentence for many.

Any time a healthcare organization is facing an audit by CMS, and sometimes commercial payers, it is a good idea to obtain an external audit by an independent source.

"It's a mistake to send off all the records to Medicare with 100% confidence that everything is correct because you have total confidence

EXECUTIVE SUMMARY

A billing audit from CMS can carry serious consequences. Understanding the process can improve the outcome.

- Always respond to audit notices promptly and fully.
- Ask an outside auditor to review the records CMS requests.
- Annual or semi-annual audits can detect problems before the government becomes involved.

in your biller who's been doing your bills forever," Kuta says. "That person only knows what they were taught. If you don't have someone from outside review at least a subset of what Medicare is asking for, you're doing yourself a disservice."

If the outside reviewer spots problems in the records Medicare requested, the organization can note that up front when submitting the documents and explain how the problem will be corrected going forward. That will show a good faith effort and may influence CMS' decision on refunds and penalties.

"I also encourage an annual or biannual audit of your billing records. It is always good to find your mistake before the government finds the issue," Kuta says. "It allows the opportunity to resolve them in an efficient manner without waiting until you're on the government's radar." ■

SOURCE

- **Christina M. Kuta**, JD, Roetzel & Andress, Chicago. Phone: (312) 582-1680. Email: ckuta@ralaw.com.

New Threats to Cybersecurity Call for Vigilance, Preparation

Cyberattacks are a major threat to healthcare organizations, with the potential for HIPAA data breaches, the loss of critical patient data, the inability to provide care, and substantial financial losses from ransoms and litigation.

The White House issued a memo to business leaders that outlines specific steps companies can take to protect against and prepare for a ransomware attack:

- Use multifactor authentication.
- Encrypt health information and other sensitive data. If data stolen during a ransomware attack are properly encrypted, the incident is not a reportable breach under HIPAA and some state laws.
- Back up data regularly, test those backups to ensure they work, and store them offline.
- Install updates and patches promptly.
- Contract with a third party to test cybersecurity strength. *(The memo is available at: https://bit.ly/3lO7Vlx.)*

Patient records are stolen in about 75% of ransomware attacks on healthcare organizations, says **Gary Salman**, chief executive officer of Black Talon Security in Katonah, NY. The thefts also include human resources, operational, and financial data.

"That poses a tremendous problem for any healthcare organization because it is double extortion. They're facing the encryption of all their files, and they can't function until they are decrypted or restored from backup, but also the threat of publishing all the stolen data," he says. "It's forcing many organizations that may have valid, recoverable backups to pay the ransom because they don't want the hacking groups to publish all of their patient records."

In some cases, the hackers will contact the patients directly if the healthcare organization will not pay the ransom, Salman says. They will tell the patient that because the hospital or physician group will not pay, the patient must give them thousands of dollars or else their personal and financial data will be sold on the black market.

The federal government and the cybersecurity industry have improved the detection of vulnerabilities in software and increased the warnings to the healthcare industry, notes **Johnny Lee**, JD, principal and practice leader in forensic advisory services with Grant Thornton in Atlanta. That is good for the industry, but likely will be necessary for the foreseeable future.

"I think we're going to continue to see regular updates about some significant software that has a vulnerability or some supply chain attack that grants malicious actors access they shouldn't have," Lee says. "What is different from a year or so ago is the coherence of the guidance coming from the federal government. It is much improved, and I think the agencies issuing guidance to covered entities are getting much better at specifics and best practice relays."

Lee says a pitfall for some organizations is the practicability of complying with the HIPAA Security Rule requirement for procedures around security incident handling. Compliance will require more than just a written policy stating the procedures.

"The rule is clear that this should contemplate both responding to the security incident and the required reporting," Lee says. "Companies that do this well have not only written it down, but they have exercised it before the bad day, so they have some muscle memory. They know they might be able to use

email if it is compromised, so they have an alternate method — things that extend well beyond a written document that looks pretty."

Patching vulnerabilities in software has become a top priority, notes **Patricia A. Markus**, JD, a partner in the Raleigh, NC, office of Nelson Mullins. Most large healthcare organizations employ good information security teams that monitor the latest patches and vulnerabilities, but smaller facilities and groups might not possess the resources.

Markus says risk managers should urge leaders to fully support information security efforts.

"It is important to be vigilant and respond promptly to the warnings from the government on these issues," she says. "Once healthcare organizations have been alerted to these vulnerabilities, it is their obligation to follow through with the recommended fixes or defense mechanisms. But it can be a real challenge for some smaller entities without the resources or expertise."

Healthcare Especially Vulnerable

Ransomware is particularly dangerous for healthcare entities, says **Scott Bennett**, JD, an attorney with Coppersmith Brockelman in Phoenix. When a healthcare entity loses access to systems or data, that can interfere with patient care. For example, it can prevent providers from accessing critical information about a patient's medical history or allergies that is stored in the electronic medical record.

"Another factor is that the need for healthcare never stops. A hospital hit by ransomware is still going to have patients showing up in the emergency department needing care, as well as patients with scheduled elective procedures," Bennett says. "That puts enormous pressure on healthcare entities to just pay the ransom so they can get on with providing patient care."

A ransomware attack also might be a reportable breach under HIPAA. The Office for Civil Rights has taken the position that if ransomware locks down electronic protected health information (PHI), that is a reportable breach unless the entity can prove there is a low probability the information has been compromised, Bennett says. Healthcare entities hit by ransomware need to think about ways they might prove that, such as through a forensic analysis of the affected devices or systems.

"Healthcare entities don't want to be thinking through issues for the first time in the midst of the ransomware attack. They need to have detailed incident response plans in place, and they need to test those plans," Bennett says. "One useful exercise is a tabletop drill where the members of the incident response team walk through a hypothetical incident. It is important to have answers ahead of time to key questions, such as how the organization will continue to operate without access to critical systems or data."

Bennett also suggests healthcare entities educate their employees about phishing emails, which are a common source of ransomware attacks. Make sure personnel know how to spot a suspicious email. They also should know what to do when they spot one (such as reporting the email to IT or security), and what not to do. They must not respond to the email, click on any links in it, or type in a username or password.

"Healthcare entities should also consider adding a highly visible label to every email that comes from an email address outside the organization, because it is increasingly common to see phishing emails that purport to be from a co-worker or boss," Bennett says.

Ransomware Attacks Prompt Concerns

The latest healthcare advisory comes after myriad ransomware attacks and other cyberthreats affecting healthcare providers, says **Morey Haber**, chief technology officer and chief information security officer at IT security company BeyondTrust. The attacks, while devasting to technology, already have proven they can delay patient care, expose sensitive health information, and, in extreme cases, cause loss of life.

"No one is immune to cybersecurity threats. When an attack is successful, it can be more than just

EXECUTIVE SUMMARY

Cybersecurity is a serious concern for healthcare organizations. The White House is urging hospitals and health systems to take specific steps to improve cybersecurity.

- Multifactor authentication is a strong deterrent to hackers.
- Updates and patches can eliminate weak points in software.
- Consider hiring a third party to test security strength.

an inconvenience or attributable to straight-up downtime," Haber says. "Sensitive information and lives are at risk."

Haber lists several cybersecurity best practices that can help healthcare organizations mitigate the risks:

• Ensure all systems are patched for critical vulnerabilities in a timely manner. This is not only true for endpoints, but also infrastructure components like hypervisors that also can be a victim of ransomware.

• Ensure end users, regardless of role, are not logging into resources with administrative privileges unless absolutely necessary. Ransomware spreads via lateral movement, and a single attack on an endpoint can compromise an entire environment.

• Ensure passwords are complex and not reused across multiple systems or infrastructure technology.

• When possible, disable legacy remote access protocols like RDP and SSH, especially with critical infrastructure. Leverage a dedicated remote access solution to mitigate the threats of protocol-based ransomware distribution. This is the highest percentage of current attack vectors.

• Consider segmenting and disconnecting from the internet any and all systems that are end of life and can no longer receive security maintenance. This includes virtual machines running on hypervisors that might hold multiple paths for access and maintenance.

Take Proactive Approach

The recent guidance from the federal government establishes additional regulations any healthcare organization must abide by to be HIPAA compliant, notes **Margaux Weinraub**, CPCU, ARM, cyber practice leader at Graham Company in Philadelphia.

The key reminder from the federal government's warning is that every organization is susceptible to cyberattacks, no matter what industry or how big or small the company. Given the nature of the industry and private medical information at stake for healthcare organizations, it is of paramount importance they take preventive measures to protect their systems and data from a cyberattack.

THE KEY REMINDER FROM THE FEDERAL GOVERNMENT'S WARNING IS THAT EVERY ORGANIZATION IS SUSCEPTIBLE TO CYBERATTACKS, NO MATTER WHAT INDUSTRY OR HOW BIG OR SMALL THE COMPANY.

HIPAA-covered healthcare entities should take a proactive approach to safeguarding their data, protecting their employees and patients and consistently reviewing their contractual obligations with outside vendors, Weinraub says. This includes contracts with third-party vendors that store or have access to the entity's personally identifiable information and PHI, which will outline insurance and indemnification provisions so risk exposure is clear and reduced to the extent possible.

"In addition, healthcare entities should be considering their organizations' security holistically," Weinraub says. "It's not just something to be addressed with IT, but from the top down as a priority that involves all employees and departments."

Update Security Constantly

Organizations should constantly update their cybersecurity measures to implement and update firewalls and operating procedures designed to prevent a breach, says **Erin McDevitt**, producer with the Graham Company in Philadelphia. This includes using multifactor authentication. A door includes both a door lock and a deadbolt, but if someone retrieves your password (or door lock), they should not be able to access all of your records (or open the door), she explains.

If an employee becomes aware of a vulnerability, he or she should be directed to acknowledge it immediately and not wait until it could become a larger issue.

"With the increase in merger and acquisition activity in the healthcare industry, it is imperative to know that organizations are most vulnerable to a cyberattack or breach while in the process of undergoing a merger or acquisition, or after its completion," she says. "An organization's risk management team and finance team must prepare for this vulnerability."

The organization's insurance broker should work closely with the executive team in the due diligence process to know the insurance provisions associated with each organization's cyber liability program and determine what coverage will be

in place upon completion of the new entity, if any tail coverage is required for the expiring programs and related issues, McDevitt says. ■

SOURCES

- **Scott Bennett**, JD, Attorney, Coppersmith Brockelman, Phoenix. Phone: (602) 381-5476. Email: sbennett@cblawyers.com.
- **Morey Haber**, Chief Technology Officer, Chief Information Security Officer, BeyondTrust, Johns Creek, GA. Phone: (877) 826-6427.
- **Johnny Lee**, JD, Principal, Practice Leader, Forensic Advisory Services, Grant Thornton, Atlanta. Phone: (404) 704-0144. Email: j.lee@us.gt.com.
- **Patricia A. Markus**, JD, Partner, Nelson Mullins, Raleigh, NC. Phone: (919) 329-3853. Email: trish.markus@nelsonmullins.com.
- **Erin McDevitt**, Producer, Graham Company, Philadelphia. Phone: (215) 567-6300.
- **Gary Salman**, CEO, Black Talon Security, Katonah, NY. Phone: (800) 683-3797.
- **Margaux Weinraub**, CPCU, ARM, Cyber Practice Leader, Graham Company, Philadelphia. Phone: (215) 567-6300.

Class Action Lawsuits Possible After Cyberattack

Class actions stemming from ransomware attacks are becoming increasingly common as the public awakens to the likelihood these episodes often are accompanied by data extradition and breaches, says **Michael J. Ruttinger**, JD, partner with Tucker Ellis in Cleveland. In the last two years, it has become increasingly common for consumers who are concerned about their own data exposure to file class actions against companies (including cloud software providers and healthcare companies).

The broadest group of potential plaintiffs are persons or other entities who learn their data have been compromised during a ransomware attack and choose to sue the company responsible for protecting that data, alleging failure to take adequate steps to protect against the attack and resulting breach.

"But it is not necessarily consumer- or even data-related. The cyberattack against Colonial Pipeline earlier this year spawned a putative class action on behalf of class members who include more than 11,000 negatively affected gas stations who were allegedly left without sufficient supply due to the attack," Ruttinger says. "Any time a group of similarly situated entities are harmed by the disruption caused by a ransomware attack, that could provide a potential basis for class action allegations."

An ounce of prevention is worth a pound of cure, Ruttinger says. Many companies already have plans in place for responding to cyberattacks and breaches. These plans can be strengthened and broadened to account for ransomware attacks. But creating a response plan is not enough. Companies should regularly test their plans to confirm their teams are ready to handle attacks and the potential fallout.

Few class actions based on ransomware attacks have progressed far enough to give a clear picture of their odds of success, Ruttinger says. However, plaintiffs in similar data breach class actions have struggled to demonstrate standing to sue. That challenge only grew with the Supreme Court's recent decision in *TransUnion, LLC v. Ramirez*, where the court substantially narrowed a class action brought against one of the nation's major credit-reporting companies involving unauthorized disclosure of personal data. *(The decision is available at: https://bit.ly/3CCR8Ij.)*

"A party seeking to succeed in a ransomware class action will likely need to be able to demonstrate a concrete injury, not just speculation about harm or an alleged statutory violation," Ruttinger says. "One of the key concerns our clients express over class actions are the lengthy and expensive discovery obligations that sometimes arise, including discovery of electronically stored information. Experienced class action counsel can often help companies streamline and navigate these challenges." ■

SOURCE

- **Michael J. Ruttinger**, JD, Partner, Tucker Ellis, Cleveland. Phone: (216) 696-4456. Email: michael.ruttinger@tuckerellis.com.

COMING IN FUTURE MONTHS

- Top risks to nursing licenses
- Hospital reduces alarms
- Responding to lawsuit threats
- Ensuring adequate ED coverage

HEALTHCARE RISK MANAGEMENT™

CME/CE INSTRUCTIONS

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

1. Read and study the activity, using the provided references for further research.
2. Log onto **ReliasMedia.com** and click on My Account. First-time users must register on the site. Tests are taken after each issue.
3. Pass the online test with a score of 100%; you will be allowed to answer the questions as many times as needed to achieve a score of 100%.
4. After successfully completing the test, your browser will be automatically directed to the activity evaluation form, which you will submit online.
5. Once the completed evaluation is received, a credit letter will be emailed to you.

CME/CE QUESTIONS

1. **According to a report from The Leapfrog Group, in what demographic did only an average of 62% give the most favorable response on how well-equipped they felt to report concerns?**

   a. Parents of pediatric patients
   b. Children of geriatric patients
   c. Women
   d. Men

2. **What does Rebecca M. Lindstrom, JD, say is a common mistake in dealing with impaired physicians and nurses?**

   a. Accepting all reports as truthful
   b. Not taking all reports seriously
   c. Providing too many treatment options
   d. Not including department leadership

3. **What does Christina M. Kuta, JD, say is a common mistake when facing a billing audit from CMS?**

   a. Failing to respond quickly and thoroughly
   b. Sending too much documentation
   c. Obtaining a third-party audit before responding
   d. Hiding negative information in records

4. **According to Gary Salman, what is one reason healthcare organizations pay ransom after a cyberattack?**

   a. The amount of money is relatively small.
   b. The hackers threaten to publish patient records.
   c. Law enforcement instructs them to pay the ransom.
   d. They cannot meet other demands of the hackers.

CE OBJECTIVES

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

1. describe the legal, clinical, financial, and managerial issues pertinent to risk management;
2. explain the effect of risk management issues on patients, physicians, nurses, legal counsel, and management;
3. 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

No Liability for Hospital Under Emergency Medical Treatment and Labor Act

*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

***Hannah S. Chacko**, LL M*
UCLA School of Law, May 2021

News: A woman brought to the emergency department (ED) died due to a stroke suffered while under the facility's care. The patient's estate sued the hospital for violating the Emergency Medical Treatment and Labor Act (EMTALA) by failing to provide her with adequate care or transfer her to another hospital.

The hospital argued it satisfied its obligations under EMTALA. The court agreed, and dismissed the case against the hospital. Although the plaintiff appealed, the determination was upheld by the appellate court, which confirmed the hospital met its obligation under EMTALA by admitting the patient to the ICU after the initial ED screening.

Background: On Aug. 3, 2016, a female patient with elevated blood pressure and weakness was transported to an ED. Upon initial screening, the hospital admitted her to the ICU for overnight care based on a concern for her cardiac condition and the potential for a stroke. The medical providers in charge were concerned the patient was "trending toward a stroke" based on neurological exams and informed the patient she could not be discharged until further tests were completed.

The patient's family inquired about transferring her to a different medical facility after an MRI showed signs of a severe ischemic stroke. A representative of the hospital had informed the patient's family that a transfer was unlikely based on the patient's care plan. Nevertheless, the patient's family provided paperwork requesting a transfer to multiple other hospitals, but those requests were denied by those other hospitals for financial and insurance reasons.

> THE PATIENT'S ESTATE ALLEGED THE HOSPITAL VIOLATED EMTALA BY FAILING TO PROVIDE ADEQUATE CARE TO THE PATIENT OR TRANSFER THE PATIENT TO ANOTHER HOSPITAL.

On Aug. 17, an apnea test (which was delayed following a request from the patient's family to be present when the result was received) revealed the patient to be clinically brain dead. The hospital ceased treatment and canceled the outstanding transfer request. The patient's family presented a written request to the hospital and received the patient's medical records.

In July 2019, the patient's estate filed suit against the hospital, expressing dissatisfaction in the quality of treatment. The complaint contained two overarching claims. First, the patient's estate alleged the hospital violated EMTALA by failing to provide adequate care to the patient or transfer the patient to another hospital. Second, the plaintiffs alleged the records the hospital provided concealed information and test results that prevented the plaintiffs from filing a timely medical malpractice action.

For the allegation of inadequate care, the patient's estate claimed the hospital violated its duties under EMTALA to screen, treat, stabilize, and transfer the patient by failing to comply with national and community standards of care. EMTALA's purpose is to prevent denial of emergency

treatment — and, in fact, discourages transfers instead of providing treatment. The court determined an emergency condition existed; thus, the patient could not be transferred to another hospital or discharged until she received stabilizing treatment. The appellate court confirmed the hospital's conduct did not violate EMTALA.

As the plaintiff acknowledged in the complaint, the hospital met the screening requirement by examining the patient and determining the emergency condition. Furthermore, the hospital met the duty imposed by EMTALA to either provide further treatment or to transfer the patient (in accordance with certain parameters) by admitting the patient into its ICU. In summary, the court confirmed the hospital met its EMTALA obligations to the patient; thus, the hospital bore no liability.

For the allegation of concealment, the patient's estate claimed certain information, paperwork, and test results were missing from the records the hospital provided. The court stated the allegations were viable only if the hospital had intentionally concealed material facts that the patient's estate could not have discovered through a reasonable inquiry or inspection.

According to the court, the patient's estate knew generally about the existence of the test results because the doctors who performed the tests told the patient or her family about them. The court determined if the patient's estate had conducted a reasonable inquiry, they could have discovered the information.

Furthermore, the court ruled the claim of fraudulent concealment rooted itself in an allegation of malpractice. In the state where these events occurred, a claim of medical malpractice is required to be accompanied by an affidavit affirming consultation with a medical expert. The patient's estate failed to provide any such documentation. The lower court and appellate court both agreed the hospital bore no liability under these circumstances.

What this means to you: This case highlights important provisions of EMTALA, which is a less common basis for allegations of improper medical care when compared to standard allegations of medical malpractice. EMTALA was enacted to prevent denial of emergency treatment regardless of ability to pay, citizenship, or legal status. It imposes obligations on medical facilities with EDs. The substantive requirements do not extend beyond the initial screening. This means EMTALA does not apply to any treatment the patient had undergone after the point of admittance or transfer, nor to the national or communal standard of care by which the patients should be treated, as EMTALA also does not specify such substantive standards.

In this case, the hospital relied on this lack of substantive provisions within EMTALA to defend against the allegations of inadequate care. The hospital appropriately provided the necessary medical screening examination to the patient when she was admitted, and actually provided treatment for the patient. The hospital did not refuse to admit or treat the patient. Its recommendation that transfer was unlikely due to the patient's status similarly did not violate EMTALA.

Since the basis of the plaintiff's allegations were not based in medical malpractice, the hospital's standard of care was not at issue in this case and was not evaluated by the court. The plaintiff claimed the hospital's failure to provide the adequate and complete records prevented a timely medical malpractice action, but the court disagreed.

Hospitals and care providers are obligated to provide a patient's medical records in a timely manner following an appropriate request. In this case, there is no indication the hospital deliberately concealed or refused to provide requested records. Such a failure would not arise to the level of medical malpractice since the provision of records is separate from the provision of medical services. It is important to provide requested records, not only because patients are entitled to such records, but also to prevent the types of allegations raised in this case where a patient attempts to circumvent an untimely claim by alleging improper concealment by the care provider.

This case also is an important reminder about how courts evaluate allegations of fraudulent concealment. Generally, a party making such allegations must assert a concealment of material information intended to induce a party into acting or refusing to act, and that party could not have discovered the information otherwise. Allegations of fraud often hold higher standards for the amount of specificity required for the initial claims to prevent parties from always claiming that the other side engaged in "fraud." It might be easier for hospitals and care providers to challenge such vague allegations of fraud early by requiring the party asserting the allegations to add specificity or concrete facts to their claims. Hospitals and care providers can eliminate frivolous fraud claims early in the litigation process to save time and effort later. ■

REFERENCE

- Decided June 28, 2021, in the United States Court of Appeals for the Seventh Circuit, Case Number 1:18-cv-5327.

Proposed Expert Witnesses Correctly Disqualified, But Proper Witness Disregarded

News: A woman died in a rehabilitation center from a pulmonary embolism two weeks after she was admitted to the facility. The patient was admitted for additional surgical procedures following a surgery to repair the infected quadriceps on her right knee.

The patient's estate filed a lawsuit against the facility, alleging the negligence of the nursing staff led to improper treatment, resulting in loss of life. The trial court dismissed the case, determining the plaintiff's expert witnesses were not qualified to testify. However, the appellate court partially reversed the trial court, finding the court had improperly excluded the testimony of the expert.

Background: On July 16, 2014, a woman died while at a rehabilitation center from a pulmonary embolism caused by a dislodged deep vein thrombosis (DVT).

According to the plaintiff, the treating physicians failed to recognize the patient's mobility was compromised while at the facility, leading directly to the failure to provide proper prophylaxis against DVT by prescribing an oral or injectable anticoagulant. Furthermore, the plaintiff claimed the nurses failed to report the patient's immobility to the relevant physician and institute a DVT prophylaxis protocol.

During litigation, the plaintiff offered testimony from three medical professionals presented as experts. However, the defendants challenged these qualifications. The court determined two of these individuals were not qualified experts for this case. Due to lack of sufficient expert testimony, the court granted a motion for judgment in favor of the defendant. The court did not attribute substantial weight to the third remaining expert.

The plaintiff appealed the decision, alleging the trial court's disqualification was improper and disregarded issues relating to causation. The appellate court considered legislative guidance on parameters for considering the qualification of expert witnesses. According to state laws, experts are required to have supervised, taught, or instructed nurses on the standard of care required under the circumstance at issue for three out of the previous five years. One of the disqualified experts expressly testified their practice involved regular interactions with nurses (including lectures), but they had not supervised nurses in more than a decade. The appellate court agreed with the trial court, noting it was the prerogative of the trial court to determine the eligibility of the expert witness — which, in this case, was inadequate.

The plaintiff claimed the second expert witness was qualified to testify, as the nurse had years of experience caring for patients at risk of DVT.However, given further scrutiny of the nurse's curriculum vitae, no testimony was provided showing the nurse possessed the knowledge and skill needed to manage a rehabilitation patient at risk of DVT. The appellate court similarly affirmed the disqualification of this proffered expert witness.

Finally, on the issue of the summary judgment in favor of the facility, the appellate court disagreed with the trial court. The trial court claimed there was nothing in the records to indicated whether the treating physician would have acted differently if informed of the patient's immobility. The treating physician's testimony influenced this conclusion when he stated he was aware of the numerous risk factors for DVT. The physician claimed he refrained from using anticoagulants because of the risks they posed. The physician testified he initially assessed the patient's risk of DVT to be low. He noted anticoagulants could amplify any injuries the patient could sustain, as she was a fall risk. The remaining plaintiff expert witness testified the patient's immobility was a significant factor for DVT, and the nurses were obligated to inform the physician.

The appellate court ruled the trial court failed to properly consider the testimony of the qualified expert witness. According to the appellate court, this determination was beyond resolution by the trial court at this stage. The plaintiff presented evidence from a qualified expert stating one position, while the defendant presented evidence to the contrary. The appellate court overruled the trial court's decision, noting the resolution of this conflicting evidence was proper for a jury to determine.

What this means to you: As often is the case, expert witnesses regularly play a pivotal role in medical malpractice actions. A foundational matter is whether an individual may qualify to serve as an expert witness. It can be extremely powerful for either party to challenge the other side's prospective experts.

There are lessons to be learned for care providers for both the offensive and defensive aspects of expert witnesses. Offensively, when a medical malpractice plaintiff presents a "weak" expert who lacks the necessary background, or perhaps who has not practiced recently, it is critical to bring a timely challenge to prevent an unqualified individual from offering inaccurate or damaging testimony. Defensively, it is important for care providers to evaluate their own prospective experts and to select individuals who are protected from such challenges. Plaintiffs are likely to bring their own attempts to disqualify experts. It is crucial to objectively evaluate a prospective expert's background and ability to testify calmly and credibly. There are numerous individuals who claim to be experts in their respective fields. While many actually are experts, not all possess the same qualifications or same ability to testify in front of a jury. Selecting the right expert, and challenging an opposing party's inadequate expert, are necessary in the vast majority of medical malpractice cases.

Courts are the "gatekeepers" when it comes to expert witnesses and their qualifications. As an initial matter, a party whose expert is challenged must sufficiently demonstrate to a trial court judge that the individual is appropriate to provide expert testimony for the issues raised in each case. A trial court judge can resolve disputes about an expert's qualifications to protect the jury from inaccurate, irrelevant, or misleading information.

In this case, the underlying issue related to DVT, and the experts provided conflicting testimony. There are many ways to prevent DVT that do not involve administering anticoagulants. Alternating pressure devices can be worn on the lower extremities to maintain a continual return of venous blood upward to the heart. Pressure hose or stockings also are available and serve much the same purpose. Decreased mobility is common for hospitalized patients, and prevention of DVT is a standard of care that is quite routine in all types of care facilities. Failure to ward off the DVT and its devastating consequences can result in a finding of negligence on the part of all professionals involved in the care of this patient.

Beyond the providence of experts, another lesson from this case is that in medical malpractice actions, the issue of causation is a regular occurrence. Unlike determining the qualifications of experts, causation is appropriately considered by a jury, not a judge. Causation is more frequently an issue of fact where both sides present different versions of events, claiming various acts and circumstances contributed to the patient's injury. Care providers regularly use expert testimony and other evidence to argue other factors contributed to the patient's injury, and the defendant care provider's actions had no effect. In this case, both sides presented conflicting positions, and it was not the court's job to resolve that dispute. This is an important procedural point, too: When a trial court exceeds its authority, care providers should consult closely with counsel to determine the proper method for reviewing and overturning that exceeded authority. ■

REFERENCE

- Decided July 1, 2021, in the Court of Appeals of Georgia, Case Number A21A0578.

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Court Rules No Private Right of Action for HIPAA, But Questions Remain

Covered entities may have found themselves breathing a sigh of relief following a recent decision from the U.S. Court of Appeals for the 4th Circuit. In *Payne v. Taslimi* (998 F.3d 648), the court ruled the plaintiff could not sue as an individual for a HIPAA violation.[1] However, the ruling is not necessarily a complete win for healthcare organizations.

The *Payne* decision reaffirmed HIPAA does not create a private right of action for the improper disclosure of individually identifiable health information, explains **Monica J. Manzella**, JD, CIPP/US, with Baker Donelson in New Orleans. Further, the judges noted every circuit court to consider that question has held that HIPAA does not create such a right (citing decisions from various other circuits).[1]

In this most recent case, the incarcerated plaintiff asserted the prison physician improperly disclosed his individually identifiable health information related to his HIV diagnosis in violation of HIPAA, as well as the 14th Amendment.

"While the *Payne* decision made clear its position on the lack of a private right of action under HIPAA, it left open the potential for a cause of action based on a violation of privacy under the 14th Amendment for the improper disclosure of individually identifiable health information," Manzella says.

She explains the 14th Amendment's protection hinges on a two-prong test: 1) whether an individual has a "reasonable expectation of privacy" in the information, which entitles it to constitutional privacy protection. If yes, then 2) whether there exists a "compelling governmental interest" in the disclosure of such information that outweighs the privacy interest.

"Focusing on the specific facts before it, the *Payne* court limited its ruling to the first prong, considering whether the plaintiff had a reasonable expectation to privacy in his HIV status while in a prison medical unit, and found he did not," Manzella says. "In reaching that conclusion, the court recognized that prison affords individuals a limited expectation of privacy, and further reasoned that whatever privacy exists after that limitation was even further diminished, considering that the medical information at issue concerned the diagnosis of and medication for HIV, which is a communicable disease."

Since it found the facts did not satisfy the first prong, the court did not consider the second "compelling governmental interest" prong.

Still Some Uncertainty

Considering the narrow holding in *Payne*, covered entities and employers must be aware that an understanding of how those two prongs will play out in future cases remains murky, Manzella says. Taking the classification of the plaintiff from the category of incarcerated to a non-imprisoned, private individual could be one factor in favor of the reasonableness of that individual's expectation of privacy.

"But even if the individual in question was an incarcerated individual similar to the plaintiff in *Payne*, what if the type of individually identifiable health information did not concern a communicable disease, or what if the information included both communicable and incommunicable disease details? Would that change the assessment of the first prong?" Manzella asks. "Moreover, the court did not consider the second 'compelling governmental interest' prong, which leaves the question open as to what would constitute such an interest that would override an individual's reasonable expectation

of privacy, assuming one exists, in the particular context of health information."

HIPAA does not expressly allow for a private cause of action, but rather the enforcement is handled by the Health and Human Services Office for Civil Rights (OCR), notes **Svetlana (Lana) Ros**, JD, partner with Pashman Stein Walder Hayden in Hackensack, NJ. Violating HIPAA comes with a hefty price tag, including a significant financial penalty to the government, and usually a requirement for a compliance program and its implementation.

Over the years, OCR has not deterred individuals from filing suit against physicians, hospitals, and other covered entities in hopes of receiving a financial payout, Ros says. The *Payne* case is the most recent example. In its *Payne* decision, the court did not address whether there was a HIPAA violation; regardless, such a violation occurrence does not automatically give the individual the right to sue, Ros explains.

"This is a positive decision for the healthcare community because it is another case that reaffirms that HIPAA does not create a private right to sue. However, the ruling on the issue of the 14th Amendment is very specific because the court only looked at the issue of privacy of a prisoner," Ros says.

Still Some Risk

In *Payne*, the court ruled there was no violation of the 14th Amendment because the prisoner lacked a reasonable expectation of privacy in his HIV status while incarcerated in a prison medical center. However, regarding covered entities living in fear of lawsuits brought by individuals, Ros does not believe they are in the clear.

"While this is a good holding for covered entities — because the court reaffirmed the position that HIPAA does not provide a private cause of action — many states have their own privacy laws, which provide for private causes of action," Ros explains. "Additionally, the finding of no expectation of privacy granted by the Constitution in this case was very limiting, as it applied to inmates. The majority of the population is not incarcerated and, thus, enjoy a much greater expectation of privacy."

Most lawsuits brought for violation of an individual's HIPAA privacy rights also include claims of either state and/or federal privacy rights, Ros notes. She anticipates that plaintiff's counsel will try to argue a viable cause of action under the 14th Amendment where there has been a disclosure of protected health information and no compelling government interest.

"Thus, it is important for covered entities to ensure that they are vigilant in staying current with HIPAA and state privacy laws and ensuring compliance," Ros says. "It is also a good idea to consider obtaining and maintaining liability insurance in case the covered entity is sued by an individual or investigated by a government agency for a potential claim of violating HIPAA." ■

REFERENCE

1. *Payne v. Taslimi*, 998 F.3d 648 (4th Cir. 2021). https://bit.ly/3y945qt

SOURCES

- **Monica J. Manzella**, JD, CIPP/US, Baker Donelson, New Orleans. Phone: (504) 566-5257. Email: mmanzella@bakerdonelson.com.
- **Svetlana (Lana) Ros**, JD, Partner, Pashman Stein Walder Hayden, Hackensack, NJ. Phone: (201) 373-2060. Email: lros@pashmanstein.com.

HIPAA Records Retention: What Really Is Required?

Risk managers and compliance officers for HIPAA-covered entities might be uncertain about what the privacy law requires regarding records retention because medical records, HIPAA records, federal laws, and state laws become entangled. Clarity on HIPAA records retention might relieve some burden so that covered entities are not doing more than necessary just to ensure compliance. The HIPAA Privacy Rule does not include medical record retention requirements, notes **Meenakshi Datta**, JD, partner with Sidley Austin in Chicago. Rather, it requires covered entities and business associates to maintain records required by their policies and procedures, such as audit logs and accounting of disclosures of protected health information (PHI), for six years from the date of its creation or the date when it last was in effect, whichever is later.

"In other words, HIPAA requires retention of programmatic HIPAA

compliance documentation," Datta says. "It has nothing to do with the retention of PHI itself."

Datta advises covered entities to evaluate the applicable federal and state requirements and develop a matrix. The matrix will include federal medical record retention requirements, as applicable, such as those for clinical laboratories as established by Clinical Laboratory Improvement Amendments of 1988, state medical record retention requirements, HIPAA compliance program record retention requirements, other federal laws that might impose document retention requirements, and risk management and medical malpractice liability considerations.

Whether a covered entity should go beyond what is required by HIPAA depends on the situation, although Datta does not necessarily advise it.

"If there are open inquiries into breaches or potential security incidents relating to a covered entity's HIPAA program or response to a prior PHI incident, there may be good reason to impose a document hold on relevant documentation," she says. "However, in the normal course, it is also important for organizations to be able to rely on their document destruction policies to avoid a scattershot approach resulting in timed-out documents physically or virtually piling up."

No Seven-Year Requirement

There is a widely perceived notion that HIPAA requires the retention of medical records for seven years, which is untrue, says **Christina Steiner**, JD, director with Alvarez & Marsal in New York City. "HIPAA requires the retention of HIPAA-related documents, but there is a distinction for electronic PHI. Because of the way it is written, some consulting agencies have interpreted that to mean that electronic PHI is included in that requirement," Steiner says. "There is some vague writing there, but it only applies to security-related documents and not electronic PHI."

State laws include their own language regarding medical records retention, and they can vary widely, Steiner notes. State laws also may not define medical records the same as federal law, so there can be confusion as how a covered entity should set its policies.

The seven-year rule can be used as a way to ensure compliance by doing more than is usually required and to simplify the rules within a single organization.

"HIPAA does not in any way, shape, or form say how long you have to house medical records, but it does say you have to have policy on medical records retention. Most state laws say six or seven years, but some have no requirement. Some covered entities choose to maintain their HIPAA records for seven years as a way to be consistent and have just one rule that applies to both medical records and HIPAA security records," Steiner says. "That effort to have one rule across the board leads to the idea that HIPAA requires the retention of medical records for a certain period, which it does not."

Another wrinkle is some covered entities include the HIPAA authorization document in the patient's medical record, rather than a separate file, she notes.

"What they've done then is to create an obligation for the six- or seven-year retention of that medical record because that's where they house the authorization," Steiner observes. "A better practice is to put the authorization in another file rather than it being a part of the medical record. If you don't want to retain the medical record for that period because your state law allows a lesser time frame, you're in a bind because you have a HIPAA authorization in there that has to be retained longer."

Other State Laws Might Apply

Covered entities with facilities in more than one state must be aware of the different state laws regarding records retention, says **Kerry Cahill**, JD, an attorney with Lindabury, McCormick, Estabrook & Cooper in Westfield, NJ.

"The covered entity has to understand who is subject to HIPAA. The entity can enter into contracts with other providers, health plans, insurance companies, health clearinghouses, as well as their business associates and subcontractors," Cahill says. "With all of these different groups, the covered entity has to identify who is subject to HIPAA. Many covered entities are contracting with electronic patient health information systems. The covered entities have to understand what records are held by all of these organizations, their legal requirements to one another, and how that affects their retention policies."

A common mistake is for healthcare organizations to focus only on HIPAA when considering privacy and records retention, says **Mark R. Ustin**, JD, partner with Farrell Fritz in Albany, NY. While it is true HIPAA does not specify how long medical records should be retained, a covered entity should not assume the

federal law is the final word on the matter, he says.

"HIPAA itself says that if a state's law is more restrictive, then that state law applies. That includes things like medical records retention requirements," Ustin says.

The HIPAA Notice of Privacy Practices should include a policy on the retention of medical records, Ustin says. Also, there should be a policy for expunging records over time, including how the decision is made to destroy records.

"The most obvious decision to make is how long you want to keep those records, and that is going to vary by the type of record, the type of entity, and applicable state laws," Ustin says. "Where possible, default to the longest minimum period required by law. Having a single period is better than having to make a decision on a record-by-record basis, trying to determine if this a record of type A or type B and which retention period applies."

Train Employees on Policy

The covered entity also should consider the statute of limitations in the state to ensure records are available in the event of a lawsuit, Ustin notes.

"Make sure you have the policies on file and incorporate this into the larger mandatory HIPAA training that you do on an annual basis to make sure your employees have a full understanding of what you've decided to do as policy," Ustin says. "It's very easy to go wrong with this because, instinctively, you might think the larger organizations will be better at this, but that's not always true. The bigger an organization is, the more complicated it is, the more likely it is that something is going to fall through the cracks."

Small and large organizations need the same basic policies and protocols, with the same baseline attention to detail, Ustin says.

Consult Applicable HIPAA Sections

For non-medical records, covered entities should consult the HIPAA requirements regarding the length of time HIPAA-related non-medical records should be retained, says **Tom Garrubba**, vice president of Shared Assessments, a group in Santa Fe, NM, that helps organizations develop best practices, education, and tools to drive third-party risk assurance.

> "WHERE POSSIBLE, DEFAULT TO THE LONGEST MINIMUM PERIOD REQUIRED BY LAW."

He says two sections under HIPAA should be noted:

- Section 164.316(b)(1) states organizations "(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity, or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment."
- Section 164.316(b)(2)(i) notes the required documentation must be retained for six years from the date of its creation, or the date when it last was in effect, whichever is later. For example, if a policy is implemented for a year before being revised, a record of the original policy must be retained for at least seven years.

Examples of non-medical records include (but are not limited to): the covered entity's policies, standards, and procedures; risk analyses; business associate agreements; breach notification documentation; contingency and disaster recovery plans; log records for viewing PHI; audits of IT systems; and physical security maintenance and update records.

"It's important to understand the distinction between medical and HIPAA-related non-medical records. The rule of thumb here is: The states set the law for medical records, while HIPAA-related non-medical documents require a minimum retention of six years," Garrubba says. "Additionally, trying to steer your way through these channels can be very risky, so ensure that you're working with your privacy and legal counsel for additional guidance." ■

SOURCES

- **Kerry Cahill**, JD, Attorney, Lindabury, McCormick, Estabrook & Cooper, Westfield, NJ. Phone: (908) 233-6800. Email: kcahill@lindabury.com.
- **Meenakshi Datta**, JD, Partner, Sidley Austin, Chicago. Phone: (312) 853-7169. Email: mdatta@sidley.com.
- **Tom Garrubba**, Vice President, Shared Assessments, Santa Fe, NM. Phone: (505) 466-6434.
- **Christina Steiner**, JD, Director, Alvarez & Marsal, New York City. Phone: (908) 572-9222. Email: csteiner@alvarezandmarsal.com.
- **Mark R. Ustin**, JD, Partner, Farrell Fritz, Albany, NY. Phone: (518) 313-1403. Email: mustin@farrellfritz.com.