HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE SINCE 1979

INSIDE

Relias Media
From Relias

DECEMBER 2021 Vol. 43, No. 12; p. 133-144

Ransomware, Other Cyber Threats Can Lead to Malpractice Cases

An Alabama hospital is facing a medical malpractice lawsuit in which parents claim their newborn child died because of a ransomware attack that shut down the facility's computer systems for eight days. If the allegations are proven, the case could mark the first death directly attributable to a ransomware attack. The case also could signal an increased risk of malpractice claims following a cyberattack.

The ransomware attack occurred in 2019. According to the lawsuit, the attack left personnel with little or no access to health records, lab results, or fetal heart rate monitoring. The lawsuit claims "the only fetal tracing that was available to healthcare providers during [the mother's] admission was the paper record at her bedside. Because numerous electronic systems were compromised by the cyberattack, fetal tracing information was not accessible at the nurses' station or by any physician or other healthcare provider who was not physically present in [the mother's] labor and delivery room. As a result, the number of healthcare providers who would normally monitor her labor and delivery was substantially reduced, and important safety-critical layers of redundancy were eliminated."

> "ONE OF THE LESSONS FROM THIS IS YOU NEED TO BE PREPARED — NOT JUST IN TERMS OF PREVENTING ATTACKS, BUT, ALMOST EQUALLY IMPORTANT, WHAT YOU DO IN RESPONSE TO AN ATTACK."

The baby was delivered with the umbilical cord around her neck, leading to severe brain damage and death nine months later. The ransomware attack had not been

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

publicly reported, and plaintiffs allege the hospital did not adequately communicate to healthcare personnel, patients, or the general public the safety risks posed by the ransomware attack. *(The lawsuit is available online at: https://bit.ly/3mUYHUR.)*

Response Is Key

The liability for the child's death likely will come down to determining the proximate cause, says **Jason Rosenthal**, JD, principal with Much Shelist in Chicago. The case will turn on the hospital's actions in not preventing the attack and how it responded during and after the attack.

"One of the lessons from this is you need to be prepared — not just in terms of preventing attacks, but, almost equally important, what you do in response to an attack. I think the liability here will turn on what the hospital knew, when they knew it, and what they did or did not disclose," Rosenthal says. "The question will be what was disclosed and whether the family might have gone to another hospital had they been provided with this information."

Hospitals and health systems should expect to be attacked, he says. Thorough and current cybersecurity protection measures remain the backbone of any defense. Rosenthal endorses the practice of periodically challenging employees with tests, such as sending an email with an unknown (harmless) attachment to see if they will open it, disregarding instructions not to do so. Employees who do click on what should be seen as a suspicious attachment should be required to undergo additional training.

Nonetheless, risk managers and other health leaders should expect their employees to make mistakes even when stringent security measures are in place, Rosenthal says. No protections are foolproof as long as human employees are involved.

"The attacks are getting more sophisticated. The greatest thing risk managers can do is to plan ahead, and that includes acknowledging that you could find yourself in this situation in which all the very good safeguards and protections you installed have been overcome and you find yourself with a significant disruption of services," he says.

This part of the plan should specify the response plan for a cyberattack in the same way most hospitals have created detailed response plans for natural disasters, fires, and other crises, Rosenthal says. There should be a detailed plan for who should be notified, who

EXECUTIVE SUMMARY

A hospital is facing a malpractice lawsuit after a ransomware attack disrupted service and data availability. The patient's death could be the first clearly caused by a cyberattack.

- Cyber insurance might not cover such litigation.
- More lawsuits could be filed alleging patient harm from a cyberattack.
- Hospitals and health systems must use a security infrastructure that minimizes patient risk from an attack.

addresses various needs and concerns, how to take networks offline, how to access backup data and who will do so, and more.

Cyber Insurance May Not Apply

Cyber insurance can offer another layer of protection, but the applicability to cases alleging patient harm from a cyberattack is unclear. Policies might offer coverage for harm caused directly to the policyholder, or they may offer third-party coverage that applies when someone else is harmed because of the cyberattack on the hospital, Rosenthal notes.

A professional liability policy also could come into play. Theoretically, a healthcare organization could draw on one or both types of insurance coverage when a patient is harmed by a cyberattack.

"Know what your cyber policy covers, and keep it handy so that when things start to happen you can refresh yourself on what is covered and who you are going to call if there is an issue," Rosenthal says. "Many of these policies ask when you're applying for the policy what kind of network controls you have in place, and the insurer requires that you maintain those protections. It is important to make sure you are staying up to date and not jeopardizing your coverage."

In the past, third-party harm from a cyberattack probably would have been covered by a professional liability policy because cyber liability exclusions were uncommon, says **Dan Hanson**, CPCU, senior vice president for management liability with the Marsh & McLennan Agency in Minneapolis. That has recently changed.

"Now that policy is likely going to have a strict cyber liability exclusion on it, meaning they are pushing all that exposure over to the cyber liability policy," Hanson explains. "If they find that 100% of the cause of bodily injury was the cyberattack, and that policy has to cover it all, I would guess there's going to be a bodily injury exclusion in that cyber policy. You potentially would have a gap in coverage."

The cyber insurance policy more commonly covers the costs of investigation, data restoration, and other expenses related to the cyberattack, but third-party damage exclusions are becoming more common and broader, Hanson says.

Similar lawsuits are likely to follow, at least in the short term, says **Thomas Finn**, director of market development for Medigate, a healthcare cybersecurity company based in St. Simons Island, GA.

"I think we will see health systems succumb to mounting regulatory-, business-, and board-driven pressures to harden their security infrastructures, and, as a result, achieve some level of protection from such liabilities in the medium to long term," Finn says. "I'm not going to argue that a patient death caused by an unreported successful breach will ultimately fall under a force majeure clause. What I'm saying is that any such future protections, insurance

Data Show Leaders Worried About Cyberthreats

Recent research shows healthcare leaders are worried about the potential consequences of a cyberattack, says **Tim Francis**, enterprise cyber lead with Travelers, an insurer based in Hartford, CT.

He notes these findings from the 2021 Travelers Risk Index: Cyber:

• **Top business concerns:** 63% say cyber, computer, technology, and data breaches are the top business concerns.

• **Top cyber concerns for healthcare leaders:**

- A security breach with someone hacking into the computer system (66%);
- Company/organization becoming a victim of cyber extortion/ransomware (63%);
- A system glitch causing a company's computers to go down (62%).

• **Managing and preventing cyber events:** In addressing these high levels of concern about cyber risk, 55% of healthcare executives say they are confident their organization has implemented best practices to prevent or mitigate a cyber event. These practices include:

- implementing firewall/virus protection (79%);
- mandating computer password updates (73%);
- creating data backup processes (71%);
- performing background checks on employees (62%).

The 2021 Travelers Risk Index: Cyber is available online at: https://travl.rs/31B0mGU. ■

coverage, and regulatory relief will all be predicated on the health system having invested in and achieved a modern standard of protection against cyberattacks."

If the health system is negligent in this respect, it will not be able to buy any protection and will not stay in business, Finn says. But if they do, they will largely be covered against such claims.

"In this case, the fact that the breach and related consequences had not been reported means the plaintiff here is highly likely to prevail," he says.

Healthcare cyber insurance underwriting and credit ratings all will be based on how up to date the health system's security infrastructure is. "Surprisingly, our government does not want to bury our health systems in penalties and liabilities," Finn says. "But everyone in the know is saying that the health systems must be part of the solution or all bets are off."

Hospitals and health systems would be wise to investigate emerging protection standards driven by federal regulations, cyber insurance, and credit bureaus. They must conduct business with all three entities anyway, so they might as well do what they can to satisfy them, Finn says.

Insurance carriers and credit bureaus — not the government — will conduct security risk assessments and point out infrastructural weaknesses that, if addressed, will lower premium costs and help address negative credit consequences.

"Health systems have nothing but positive reinforcement around making the right investments to harden their security. A hardened security infrastructure is operationally more efficient and is cost-effective from an insurance, credit, and potential fines or penalties that the government would seek to collect," Finn says. "Health systems also should learn how to scope their attack restoration costs. Assuming they do get hit, how much coverage do they need, and where do they need relief? Amazingly, most health systems really don't understand the extent of the damage caused by a successful breach."

> "AMAZINGLY, MOST HEALTH SYSTEMS REALLY DON'T UNDERSTAND THE EXTENT OF THE DAMAGE CAUSED BY A SUCCESSFUL BREACH."

A firm policy of never paying ransom is feasible only if the government guarantees restoration cost coverage, says Finn, who does not see this happening.

"I do see some combination of public and private relief coalescing, but that will be dependent on the quality of the health systems defenses," he says. "In other words, there is no solution for the health system that will work if they don't wisely invest in their security infrastructures."

The fact the breach went unreported "was nuts. Hard to believe," Finn says. The hospital did not immediately report a HIPAA breach, and issued a press statement acknowledging a security incident a week into the ransomware period, on the day the plaintiff delivered her baby. The plaintiff alleged she did not know of any cyberattack or compromised operations when she entered the hospital.

The breach of protected health information (PHI) poses a serious liability risk, aside from any patient safety issues related to the attack, Finn says. About one-third of healthcare facilities hit by ransomware will pay the ransom, and data access will be restored by the cybercriminal in 69% of those cases, Finn says. Those organizations usually think that means they are protected from lawsuits.

"Of course, they're not. This scenario just played out in Massachusetts" after a cyberattack breached PHI, Finn says. "The plaintiff lawyers said payment of the ransom was an admission of guilt, and they would not accept the word of the cybercriminal as evidence that stolen patient data had been destroyed."

Hospitals and health systems must harden their security infrastructures and protect themselves from cyberthreats, be immediately transparent about any breach or disruption, and always must demonstrate they are doing everything they can to prevent cyberattacks.

"If a hospital behaves in this way, they will be best positioned to deal with the restoration costs and move on. If they don't, they leave themselves open to fines, fees, and astronomical, untold liabilities," Finn says. ■

SOURCES

- **Thomas Finn**, Director, Market Development, Medigate, St. Simons Island, GA. Phone: (855) 908-0775.
- **Dan Hanson**, CPCU, Senior Vice President, Management Liability, Marsh & McLennan Agency, Minneapolis. Phone: (763) 548-8599. Email: dan.hanson@marshmma.com.
- **Jason Rosenthal**, JD, Principal, Much Shelist, Chicago. Phone: (312) 521-2437. Email: jrosenthal@muchlaw.com.

Circuit Court Decision Could Make COVID-19 Lawsuits Easier

A recent federal appeals court decision appears to put nursing homes at risk of lawsuits related to deaths of patients during the COVID-19 pandemic. It also might increase the risk for other healthcare entities.

The U.S. Court of Appeals for the 3rd Circuit held that nursing homes were not protected by the 2005 Public Readiness and Emergency Preparedness (PREP) Act in the way they thought, explains **Drew Graham**, JD, partner with Hall Booth Smith in New York City.

One aspect of the PREP Act limited liability for healthcare unless plaintiffs could show "willful misconduct" in causing the alleged injuries, Graham explains. Even when willful misconduct was alleged, those were to be transferred to a federal court in Washington, DC. However, the recent 3rd Circuit ruling says if no willful misconduct is alleged, and the claim is for ordinary negligence, those cases belong in state court.

The result is nursing homes might be subject to far more COVID-19 claims than they thought, Graham says. Other healthcare entities also might have reason to worry.

"One of the things we are concerned about is this being a 'nursing homes first' situation. With all the attention being on nursing homes right now, potentially this could involve other healthcare organizations," Graham says. "As interpretations of this ruling begin to solidify, we are concerned that it might be an interpretation that is fully inconclusive of the hospital, allied institutions, pharmacies, first responders."

As the first appellate decision on this issue, the 3rd Circuit's ruling could affect three other pending cases that hinge on interpretations of the PREP Act, Graham says. Much of the risk to healthcare entities comes from the lack of consistency if COVID-19-related cases are not handled at the federal level.

"If the interpretation becomes inconsistent from state to state or county to county, it could potentially impact all individuals who participated in the disaster response, everyone who would be covered by the PREP Act," Graham explains. "This has been characterized as a nursing home issue, but I don't see any limitation by the 3rd Circuit that means it couldn't be applied in the same way to a hospital or other healthcare organizations."

There might be more concern as state protections enacted for COVID-19 begin to expire.

"The big takeaway is that the appellate court interpretation of the PREP Act has begun, and we expect it to pick up steam in the next two to three months," Graham says. "If you have not been following it, now is the time to start paying attention to what the court limitations are likely to be. Ultimately, it looks like it will be state court judges who decide the interpretation of that act." ■

SOURCE

- Drew Graham, JD, Partner, Hall Booth Smith, New York City. Phone: (212) 805-3632. Email: dgraham@hallboothsmith.com.

CMS Requires COVID-19 Vaccinations for Healthcare Workers

The Centers for Medicare & Medicaid Services' (CMS) highly anticipated interim final rule requiring healthcare workers to be vaccinated against COVID-19 will bring new obligations for healthcare employers, but it also might help overcome the objections of some employees.

The rule was released along with OSHA's interim final rule requiring vaccination or weekly testing for COVID-19 for employers with 100 employees or more, which also may apply to certain healthcare employers covered under the CMS rule, says **Carly O. Machasic**, JD, attorney with Clark Hill in Detroit.

The main difference between the two vaccination mandates is there is no weekly testing option for healthcare workers, she says. The rule is expansive in terms of scope and covers a wide range of workers in healthcare settings that receive Medicare or Medicaid reimbursement, including, but not limited to, hospitals, dialysis facilities, ambulatory surgical settings, and home health agencies, Machasic says. The categories of individual

workers covered by the rule also are broad and include not only licensed practitioners, but students, volunteers, trainees, administrative staff, leadership, and any other individuals providing care, treatment, or other services, regardless of clinical responsibility, relationship to patient care, or work location.

The only exception is for individuals who work 100% remotely or provide one-off non-healthcare-related services.

"While healthcare employers have known for months that this vaccination mandate was coming, we now finally have answers about the timeline for compliance," Machasic explains. "Within 30 days of the announcement, covered healthcare employers must require workers to receive their first dose." *(The interim rule can be found online at this link: https://bit.ly/3knao4W.)*

January Deadline

A statement released by the White House explains healthcare employees will need to receive their final vaccination dose — either their second dose of Pfizer or Moderna, or single dose of Johnson & Johnson — by Jan. 4, 2022.

"OSHA also is clarifying that it will not apply its new rule to workplaces covered by either the CMS rule or the federal contractor vaccination requirement. Both OSHA and CMS are making clear that their new rules pre-empt any inconsistent state or local laws, including laws that ban or limit an employer's authority to require vaccination, masks, or testing," the statement says. *(The statement is available at: https://bit.ly/3n0EI7b.)*

The requirements were originally set forth in President Biden's Path Out of the Pandemic COVID-19 Action Plan in September 2021, Machasic says.

"Many of the covered healthcare facilities were among the first to require COVID-19 vaccinations for employees by their own volition, but now requiring COVID-19 vaccinations will be a condition of federal funding under Medicare and Medicaid," she says.

The White House indicated the goal is to "create a consistent standard across the country, while giving patients assurance of the vaccination status of those delivering care." *(More information is available online at: https://go.cms.gov/3obmU8F.)*

Expect Progressive Enforcement

In the rule, CMS also emphasized the purpose is to protect patients and those who receive care and services by healthcare workers, Machasic says. The vaccination mandate is expected to affect more than 17 million healthcare workers.

CMS has indicated affected healthcare employers should expect a "progressive pattern of enforcement and remedies," Machasic notes.

"The rule is largely silent on specific penalties for noncompliance but indicates that interpretive guidance will be released on this issue. The rule states that CMS will consider all penalties available under federal law, including civil penalties and disenrollment," she says. "Unfortunately, the rule offers little guidance in terms of handling requests for religious accommodation. While CMS makes clear that healthcare employers are expected to provide medical and religious accommodations consistent with federal anti-discrimination laws and must document the process and decision, CMS does little to address the procedure for handling exemptions, particularly given the unique environment of healthcare."

Healthcare facilities that have already implemented vaccine mandates have seen a flood of exemption requests, particularly for religious reasons, Machasic says. In the past, healthcare facilities have not seen anywhere near the same volume of accommodation requests with other vaccination programs, like annual influenza vaccination, which has been standard for healthcare workers.

Many healthcare employers have taken the position that any accommodation request requiring exemption from the COVID-19 vaccination by frontline workers is an undue burden and poses a direct threat to the health and safety of patients and other frontline workers, given the nature of the pandemic and particularly the delta variant, Machasic says. CMS merely refers to updated guidance issued recently from the Equal Employment Opportunity Commission (EEOC)

EXECUTIVE SUMMARY

The Centers for Medicare & Medicaid Services requires healthcare employees to receive COVID-19 vaccinations by Jan. 4, 2022. Weekly testing is not an option.

- The rule says little on specific penalties for noncompliance.
- Expect more litigation regarding vaccination exemptions.
- Employers may use the rule to overcome vaccine hesitancy.

on religious objections to COVID-19 vaccine mandates.

"Notably, in that updated guidance, the EEOC did indicate that employers working with 'medically vulnerable individuals' may take that into consideration when determining whether an employee's request for an exemption from the mandate is an undue burden," Machasic says. *(The EEOC guidance is available at: https://bit.ly/3n0HHfT.)*

More Vaccine Litigation Likely

Litigation over religious accommodations related to vaccination exemption has largely been dormant until the COVID-19 pandemic, Machasic says. Now, there are several pending lawsuits against healthcare facilities that likely will flesh out an employer's obligation relating to exemptions.

"With the broad-sweeping nature of this rule, we would expect to see more litigation on this front into 2022," Machasic says. "But this does little to help healthcare employers now as they review religious exemption requests."

Regarding medical accommodations, Machasic says the rule is more explicit regarding what information employers are required to gather from individuals seeking a medical exemption, including specific information about the contraindication for the specific COVID-19 vaccine. Up to now, many employers have been using more generic medical accommodation paperwork, Machasic says, but the rule requires healthcare employers to take a more targeted approach to requests for medical accommodation.

With healthcare workers in short supply, Machasic says the potential loss of workers because of a vaccination mandate is top of mind for healthcare employers.

"In its commentary, CMS acknowledges this issue. However, CMS emphasizes that many large healthcare systems among the first to implement vaccine mandates have largely seen widespread compliance, not mass resignation," she says. "Many healthcare facilities cannot absorb even a relatively small decrease in staff, so staffing will remain an ongoing concern for many healthcare employers. Healthcare employers are hopeful that consistency among the industry with respect to vaccine mandates will offset the impact that voluntary mandates may have had prior to the rule. Simply, if healthcare workers want to stay in the industry, vaccination is required." ■

SOURCE

- Carly O. Machasic, JD, Clark Hill, Detroit. Phone: (313) 309-6996.

Civil Cyber Fraud Initiative Will Increase Some Liability Risk

A new Department of Justice (DOJ) initiative intended to hold government contractors accountable when they fail to meet required cybersecurity standards could lead to increased risk from the False Claims Act (FCA) for healthcare entities.

In announcing the Civil Cyber-Fraud Initiative, Deputy Attorney General **Lisa Monaco** stated the DOJ "will utilize the False Claims Act to pursue cybersecurity-related fraud by government contractors and grant recipients." *(The announcement is available online at this link: https://bit.ly/3BTLgsh.)*

The Civil Cyber-Fraud Initiative is intended to address government contractors and others who receive federal funds when their cybersecurity practices or protocols fall short of government requirements. The DOJ is pursuing companies and individuals who knowingly misrepresent their cybersecurity practices and who fail to properly report cybersecurity breaches, says **Paul F. Schmeltzer**, JD, an attorney with Clark Hill in Los Angeles.

"Healthcare organizations maintain protected healthcare information in a lot of ways, but mostly that information is held through third-party vendors. This initiative has the potential to impact not only the healthcare organization but also the third-party vendors that maintain this data for them," Schmeltzer says. "If the healthcare entity is receiving federal funds through Medicare or Medicaid and there is a cybersecurity incident, they could be implicated by the fraud initiative if they do not maintain a robust vendor management program."

Some Vendors Lie About Security

It is not unusual for third-party vendors to claim on paper they have certain cybersecurity measures in

place when in reality they do not regularly implement and update them. "That is where the biggest concern should be for a healthcare organization. If you have a third-party vendor, whether that is your electronic health record [EHR] vendor or a pharmacy management vendor, and they are not securely maintaining PHI when a security incident like ransomware occurs, the healthcare organization could be implemented under this fraud initiative," Schmeltzer says.

Schmeltzer advises conducting a vendor management review at least annually and preferably every six months, "just to keep them honest." That involves reviewing security measures and asking the vendor to attest in writing as to what security measures they have in place, then determining if these claimed security measures meet the government's criteria.

If the healthcare entity is found liable under the initiative, the potential losses are the same as for any liability exposure under the FCA — easily hundreds of thousands of dollars, Schmeltzer says.

Using FCA as Big Stick

The DOJ is making clear it is implementing the FCA — and particularly the whistleblower provision — in its fight against cyber threats, forcing healthcare organizations to use the necessary safeguards and ensure they only work with vendors who do the same, says **Kathleen McDermott**, JD, partner with Morgan Lewis in Washington, DC. She previously served as an assistant U.S. attorney and DOJ healthcare fraud coordinator.

McDermott calls the initiative a "prominent, high-profile, aggressive" move by DOJ. The initiative is well staffed, and she expects to see some immediate action against offenders.

"There is a host of terms and definitions that will be introduced into contracts going forward. For a government contractor, this is a very big deal in terms of compliance," she says. "The fact they're emphasizing whistleblowers is a bit different institutionally for DOJ, but they are asking whistleblowers to come forward because it is such an area of technical complexity and sophistication that they're not going to understand the noncompliance and vulnerability unless experts come forward to help."

In some ways, the healthcare industry is far ahead of other government contractors in complying with cybersecurity standards because it has been governed by HIPAA and the Health Information Technology for Economic and Clinical Health Act for so many years, McDermott says. Nevertheless, the DOJ initiative creates added pressure on healthcare entities.

McDermott advises healthcare organizations to presume the DOJ initiative is the starting bell for improving cybersecurity practices. "This does affect healthcare, even if you are subject to the Federal Acquisition Regulation [FAR] because one of your contractors may be. If anything about your cybersecurity is questionable, now is the time to upgrade," she says. "Using the False Claims Act and the Whistleblower Act creates a heightened exposure, so you're going to see an uptick in cyber reporting and an uptick in subpoenas related to this."

The DOJ's announcement was made in the context of a broad and overdue federal effort to improve the government's cybersecurity, says **David Hall**, JD, partner with Wiggin and Dana in Philadelphia. Previously, Hall served for more than 20 years as a federal prosecutor with the DOJ.

The FCA has been used before in the cybersecurity context, and such FCA actions commonly originate in whistleblower complaints. "While itself not a new source of FCA liability, the DOJ announcement is an important statement of DOJ priorities with important risk implications," Hall says. "The DOJ statement is a sign that cybersecurity enforcement using the FCA is a priority for DOJ. More whistleblower complaints are likely after DOJ's announcement."

U.S. attorneys will be more likely to intervene in qui tam actions. "This means that compliance risk increases because the chances of becoming involved in an enforcement action increases," he says. "DOJ is, in effect, reminding government contractors of the importance of an effective and proactive compliance program."

Government contractors should ensure their certifications and disclosures to the government are accurate,

EXECUTIVE SUMMARY

The U.S. Department of Justice (DOJ) is pursuing an initiative aimed at uncovering and punishing government contractors with insufficient cybersecurity or who fail to report breaches. The agency is wielding the False Claims Act as a primary tool.

- DOJ is encouraging cybersecurity whistleblowers.
- Vendors often claim to have better cybersecurity than they do.
- The initiative may be challenged in court.

Hall says. It also is important that disclosures to the government are complete and do not omit material information.

The federal government is focused on combating new and emerging cyber threats, says **Michael J. Waters**, JD, partner with Polsinelli in Chicago. This initiative demonstrates a recognition by the government that it cannot combat these threats alone and needs the cooperation of the public sector, including government contractors.

"If the government feels that it is not getting sufficient cooperation, it may utilize the False Claims Act to effectuate change. That poses a risk for government contractors, who must ensure that they are taking sufficient steps to protect data, be forthright in their claims regarding the state of their cybersecurity, and comply with security incident notification obligations," he says. "Risk managers should take multiple steps in response to the initiative, including ensuring that their organizations have implemented the Cybersecurity Maturity Model Certification framework and other required cybersecurity protections, review the accuracy of security-related representations and warranties in public-facing documents and government contracts, and make sure they understand their notification requirements so they are prepared to comply with those requirements in the event of a data incident."

The initiative is likely to face challenges in the courts, says **Michael F. Dearington**, JD, associate with Arent Fox in Washington, DC. He notes the Supreme Court explained in *Universal Health Services, Inc. v. United States ex rel. Escobar*, (2016), the FCA is not "a vehicle for punishing garden-variety breaches of contract or regulatory violations." *(The decision can be found at: https://bit.ly/3qqVazy.)*

Government contractors faced with FCA suits could contend the government and whistleblowers cannot use the FCA to punish what arguably amount to regulatory violations, Dearington explains. Whether such suits are viable likely will depend on whether compliance with cybersecurity requirements is material to the government's payment decision.

The initiative already is being tested in the courts, Dearington says. In *United States ex rel. Markus v. Aerojet RocketDyne Holdings, Inc.*, a former cybersecurity employee at aerospace contractor Aerojet RocketDyne Inc. (AR) accused AR and its holding company of fraudulently obtaining billions of dollars of NASA contracts and subcontracts while failing to maintain mandatory FAR and Defense Federal Acquisition Regulation Supplement cybersecurity requirements, in violation of the FCA.

The district court denied AR's motion to dismiss for lack of materiality in 2019, and the parties recently filed cross-motions for summary judgment. The DOJ filed a Statement of Interest on challenging AR's argument that noncompliance with cybersecurity requirements is immaterial, Dearington notes.

The district court's ultimate decision could provide an indication of how courts will react to cases brought under the initiative, and whether a defendant can commit fraud by obtaining contract payments while failing to maintain adequate cybersecurity standards, he says. *(The decision is available at this link: https://bit.ly/3n442sW.)* ■

SOURCES

- **Michael F. Dearington**, JD, Associate, Arent Fox, Washington, DC. Phone: (202) 715-8495. Email: michael.dearington@arentfox.com.
- **David Hall**, JD, Partner, Wiggin and Dana, Philadelphia. Phone: (215) 988-8325. Email: dhall@wiggin.com.
- **Kathleen McDermott**, JD, Partner, Morgan Lewis, Washington, DC. Phone: (202) 739-5458.
- **Paul F. Schmeltzer**, JD, Clark Hill, Los Angeles. Phone: (213) 417-5163. Email: pschmeltzer@clarkhill.com.
- **Michael J. Waters**, JD, Partner, Polsinelli, Chicago. Phone: (312) 463-6212. Email: mwaters@polsinelli.com.

2021 Healthcare Takedown Shows DOJ's Focus on Pandemic

The Department of Justice's (DOJ's) 2021 Healthcare Takedown report indicates government investigators are looking for fraud in some areas related to the pandemic as well as some perennial sources of wrongdoing.

Known in the industry as the Healthcare Takedown, DOJ's annual announcement of healthcare fraud indictments across the country has the primary purpose of showing its commitment to fighting fraud, explains **Lawrence J. Cameron**, JD, partner with McGuire Woods in Raleigh, NC. But the annual announcement can be analyzed for a look into where the DOJ and U.S. attorneys are focusing their efforts to find and punish healthcare fraud.

Four Types of Fraud

The 2021 report includes charges against 138 defendants, including 42 medical professionals, involving allegations of $1.4 billion of fraud involving federal healthcare programs. That is a sharp drop from the 345 defendants charged with $6 billion in fraud in the 2020 Healthcare Takedown. (*The 2021 report is available online at: https://bit.ly/3wjjepd.)*

The DOJ focused on four types of fraud in 2021. The largest amount of fraud loss charged involved telemedicine, possibly because of the greatly increased use of this technology during the COVID-19 pandemic. The DOJ charged 43 defendants with more than $1.1 billion related to telemedicine fraud.

Charges related specifically to COVID-19 accounted for $29 million in false claims to federal healthcare programs. Sober homes were cited for $133 million in illegal conduct, such as paying kickbacks to referring providers and billing for medically unnecessary care. Continuing from previous years, the DOJ focused on opioids, charging 19 defendants who prescribed 12 million doses of opioids and other narcotics and submitted $14 million in false claims.

Cameron notes 42 of the 138 defendants charged in 2021 were licensed medical professionals. One example involved a physician, physician assistant, and a nurse practitioner who the DOJ says operated a "pill mill," distributing approximately 150,000 illegal prescriptions.

"Prosecutors alleged that they prescribed large quantities of prescription opioids, benzodiazepines, sleeping medications, and muscle relaxers to people who essentially were addicts, without even providing a medical exam first," Cameron explains. "Most of their patients paid cash, but the defendants allegedly continued to bill Medicaid, Medicare, and private insurance at least sometimes for the same patients."

The DOJ estimates such illegal prescriptions have cost Medicare approximately $5.7 million since 2017, according to the report.

COVID-19 Fraud on Radar

Some of the 2021 prosecutions were influenced by funds that flowed into the federal system because of legislation intended to address the COVID-19 pandemic.

"DOJ is focusing on anything that can even tangentially be related to COID-19 fraud. You have telemedicine and sober homes because there was an increase in addictive behavior during the pandemic, so it's not just the direct fraud related to relief funds," Cameron says. "The surprise was that it was a bit smaller than last year's takedown."

Cameron suspects the smaller number was due to the DOJ focusing on pandemic-related cases, even if that meant the number of prosecutions would be smaller, with the goal to send a message that would deter future profiteering from COVID-19.

"They're trying to deter [fraudulent] conduct. They're being more targeted and showing that they are going to regularly and aggressively target offenders in this area to deter bad actors," Cameron says. "The message for risk managers is that the sooner you can catch a bad actor who may be involved with your organization, the better. The sooner

EXECUTIVE SUMMARY

The Department of Justice's annual report shows a focus on telemedicine and COVID-19 fraud. The number of charges and defendants dropped form 2020.

- Telemedicine was involved in $1.1 billion of fraud.
- Sober homes and opioid prescriptions accounted for many charges.
- About one-third of defendants were licensed medical professionals.

you can get in front of it and self-report, the better you are going to come out of it in the end."

The issues the DOJ focused on this year probably will carry over into 2022 enforcement, Cameron says. Telemedicine is one area that could receive even more attention.

"During the pandemic, some of the requirements around telemedicine were loosened. Now, there is some expectation that some of the pre-pandemic restrictions will be back into play," Cameron says. "Healthcare organizations need to be mindful about how they are monitoring the regulations and how they adjust their internal policies and procedures so they are compliant if some of these pre-COVID requirements come back." ■

SOURCE

- **Lawrence J. Cameron**, JD, Partner, McGuire Woods, Raleigh, NC. Phone: (919) 755-6601. Email: lcameron@mcguirewoods.com.

Co-Branding Requires Attention to Anti-Kickback, Stark, Tax Laws

Co-branding is a common tactic in healthcare that signals collaboration, excellence, and high-quality service offerings. But as common as co-branding is, healthcare providers that use this must have a legal structure in place as the integration occurs.

Risk managers must be careful to keep their organizations from violating the Anti-Kickback Statute, Stark Law, and tax laws while engaged in a co-branding arrangement, says **Jeanna Palmer Gunville**, JD, shareholder with Polsinelli in Chicago. The issue is becoming more common as health systems seek to bring more providers under their umbrella.

A system's brand name often is the biggest asset they bring to the table when negotiating partnerships, Gunville says. But leaders sometimes question how they want to use the brand name and what is involved with doing so.

"Are we setting a precedent with putting a value on it if we use it in this transaction? If we allow the use of our brand, how protected can we make the use of it, and how do we unwind it if clinical parameters and quality measures are not met?" she asks. "All of those parameters are very important to consider on the front end, and it helps you know when to engage a valuation consultant in the process."

When faced with a potential co-branding opportunity, risk managers should consider how extensive the arrangement would be and any limits that might be imposed. Determine what kind of relationship is being considered — a limited use of the brand or a full partnership?

Establish quality indicators that must be met, and the process for withdrawing the brand if those metrics are not met. Determine what usage of the name, logo, and other branding is allowed.

"What incidents would be immediately reportable and make you reconsider how you will allow usage of the brand? Risk managers are very close to the ground and have a good feel for what kind of things will have a real impact on how the brand is perceived by the public," Gunville says. "Work with your attorney to spell out these expectations and how you will hold the other party accountable."

The risk manager also must address potential fraud and abuse exposure as well as tax law liabilities.

"When using your brand and assigning a value to it, you must be sure it is licensed at fair market value. To not do that raises compliance issues with the Anti-Kickback Statute, the Stark Law, and tax laws applying to tax-exempt organizations," Gunville says. "When you are looking at assigning a value to the brand, it's important that it is supportable through an evaluation consultant's report backing up the fair market value assigned to the brand." ■

SOURCE

- **Jeanna Palmer Gunville**, JD, Shareholder, Polsinelli, Chicago. Phone: (312) 873-2950. Email: jgunville@polsinelli.com.

COMING IN FUTURE MONTHS

- Physician recruiting agreements
- Controlling workplace violence
- Changing risks of telemedicine
- Reducing workers' comp claims

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. **What is a likely result of the U.S. Court of Appeals for the 3rd Circuit regarding nursing homes and the 2005 Public Readiness and Emergency Preparedness Act?**

   a. Nursing homes will be less vulnerable to lawsuits related to care provided during the COVID-19 pandemic.
   b. Nursing homes will be more vulnerable to lawsuits related to care provided during the COVID-19 pandemic.
   c. Nursing homes will be "virtually immune" to lawsuits related to care provided during the COVID-19 pandemic, but other healthcare entities will be more vulnerable.
   d. Nursing homes will be more vulnerable to lawsuits related to care provided during the COVID-19 pandemic, but other healthcare entities will be "virtually immune."

2. **What is the date by which healthcare employees must have their final dose of a COVID-19 vaccine?**

   a. Jan. 4, 2022
   b. Jan. 30, 2022
   c. Feb. 4, 2022
   d. Feb. 28, 2022

3. **Which is one of the allegations in the case involving a medical malpractice lawsuit against an Alabama hospital after a ransomware attack?**

   a. The hospital did not notify the public that hospital services were compromised by the ransomware attack.
   b. The hospital refused to reduce the family's medical bills after acknowledging the ransomware attack.
   c. The hospital notified the plaintiffs it was experiencing a ransomware attack, but assured them that no services were compromised.
   d. The hospital unlawfully released protected health information regarding the patients when reporting the ransomware attack.

4. **What is one area the Department of Justice focused on for fraud investigations in 2021, according to the 2021 Healthcare Takedown report?**

   a. Mergers and acquisitions
   b. Telemedicine
   c. Chiropractic medicine
   d. Pharmacy management

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

Fraudulent Concealment Prevents Physician from Using Statute of Repose Defense

*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 patient presented several times to the same hospital with complaints of abdominal pain. Multiple CT scans revealed a kidney mass. A physician was informed of the radiology recommendation to follow up, but the patient was not informed of the mass until 12 years after the initial discovery. The mass eventually was diagnosed as cancerous, and the patient later passed away.

The patient initiated a lawsuit before she passed, alleging malpractice and fraudulent concealment by the defendant care providers. The care providers denied liability and argued the suit should be barred because it was untimely. A trial court initially agreed, but an appellate court reversed, determining a genuine issue about the alleged fraudulent concealment sufficient to defeat the medical professionals' defense.

Background: In 2004, a woman underwent a CT scan that revealed a kidney mass, but neither the patient nor her family were notified of the mass. In 2006, the patient sought treatment at the same hospital for a urinary tract infection. Another CT scan was taken and the mass was observed, yet no information was provided to the patient or her family.

On Oct. 1, 2009, the patent was admitted to the same hospital's emergency department (ED) with a complaint of abdominal pain. She was examined by a physician and underwent a CT scan. The physician initially claimed the scan looked normal, but revised that diagnosis hours later. The physician asked the patient to return to the facility as further review caused the medical professionals to conclude "not everything is OK." When the patient returned, she was diagnosed with colitis and received a prescription for an antibiotic before going home again. The CT scan taken at this visit showed the kidney mass had grown since the 2004 and 2006 scans, yet the patient still was not informed about the potentially problematic mass. The discharge instructions from the hospital did not mention the kidney mass.

A PHYSICIAN WAS INFORMED OF THE RADIOLOGY RECOMMENDATION TO FOLLOW UP, BUT THE PATIENT WAS NOT INFORMED OF THE MASS UNTIL 12 YEARS AFTER THE INITIAL DISCOVERY.

Two days later, the patient returned to the ED with the same complaint of abdominal pain. Another CT scan was performed. This time, the physician was informed of the radiology recommendation to follow up on the mass to ensure it was not cancerous. On Oct. 6, 2009, the same consulting physician wrote a letter to the patient's primary physician detailing his treating her for colitis, and failed to mention the kidney mass. After two months, the consulting physician discharged the patient from his treatment.

On April 24, 2016, the patient was admitted to the same hospital's ED due to a broken arm, and yet another CT scan revealed the kidney mass. The patient was referred to a different hospital for treatment of her arm. During discharge from the original hospital, a nurse mentioned

the kidney mass to the patient, which was the first time the patient had ever been informed of the mass that was initially observed in 2004. Later that year, the patient was diagnosed with metastatic renal cell carcinoma. She passed away approximately three years later.

Before her death, the patient filed a lawsuit against multiple individuals and entities, including the initial hospital and physician. Her daughters substituted after their mother passed. The defendants brought a motion for summary judgment prior to trial, arguing the patient's action was barred for being untimely under what is known as a statute of repose. The defendants argued the alleged negligence occurred in 2009, but the litigation was initiated in 2018. Based on a state statute, litigation for personal injury or wrongful death against a physician must be brought within six years.

The patient's estate claimed their case fell within an exception to this requirement based on the medical providers' fraudulent concealment of the negligence, since the patient had not been informed of the mass until 2016. The trial court granted the defendant medical providers' motion, and the patient's estate appealed. The appellate court disagreed with the trial court and found a genuine issue about the alleged fraudulent concealment sufficient to defeat the defense. The matter was sent back to the trial court for further proceedings.

What this means to you: This case reveals the importance of providing patients with relevant information and documenting the provision of information in a timely fashion. In this case, the negligence focused on the physician's failure to inform the patient about the kidney mass and failure to diagnose the cancer. Patients must be allowed to make fully informed decisions. When patients are not fully informed of material information, such as an abnormal mass, patients are deprived of that ability. The patient in this matter claimed she was not informed of the mass until 2016, even though it was initially observed in 2004. That is a huge gap of time, during which multiple scans were taken. Multiple care providers must have seen the images revealing the mass, yet the patient was never informed.

Unfortunately, this set of facts is an all-too-familiar scenario that results in medical malpractice actions. A patient presents to a physician's office or ED on multiple occasions with the same complaints, and the patient is discharged with a convenient and uncontroversial diagnosis (in this case, colitis). But such a diagnosis and discharge might not be sufficient, particularly when the patient reappears with the same complaints after undergoing treatment for the initial diagnosis. Upon presentation the second or third time, the applicable standard of care might require the physician or care provider to re-evaluate the initial diagnosis and perform additional testing to determine whether there is a different diagnosis; perhaps a rarer condition is at issue, or additional imaging could provide new information to better diagnose the patient.

Consultation with other physicians or other departments could provide useful insight as well. Obtaining a second or third opinion can allow another individual to identify something the initial physician might have missed — or may simply confirm the initial diagnosis, in which case the initial physician has gathered a useful level of protection in the event of a subsequent malpractice action. The physician in this case was even informed of the radiology recommendation to follow up. Reviewing imaging with a radiologist would have undoubtedly helped the physician in this matter to understand the proper diagnosis and to timely diagnose the patient's cancer.

Beyond actually informing patients of necessary information, it is important to accurately and thoroughly document what the patient has been told, and when. Providers must maintain clear records not only to facilitate treatment, but also to protect against claims of malpractice wherein a patient claims he or she was not informed. One challenge of these circumstances is precisely these large gaps of time. It takes years for a medical malpractice action to proceed through the legal process, and even the beginning of that process could be several years after the underlying treatment or injury.

By the time four or five years have passed, it is natural for memories to fade. Keeping a written record — ideally, signed by the patient confirming he or she received the information — is extremely valuable to prove the physician or care provider informed the patient of material facts, or of risks associated with a procedure. It may seem tedious or difficult to carve time out from treatment to maintain and document events, but keeping a regular practice of documentation and obtaining a patient's informed written consent might prove to be the critical factor in defending against a malpractice action.

Another important takeaway from this case relates to legal provisions barring old matters, which are known

as statutes of limitations and statutes of repose. While there are differences between the two, the function is similar: If applied, the statute prevents liability because the matter should have been brought within a specified period. These statutes vary from state to state, but all states have versions of these to encourage parties to act within the set period and to provide some certainty to individuals that they will not be pursued 10 or 20 years later.

Statutes of repose, such as the one raised in this case, are particularly powerful defensive tools because the statute bars a late claim even if the plaintiff was not injured or did not know he or she was injured at the time. In this case, the underlying malpractice occurred almost 10 years before the patient filed suit, but the patient was unaware of the malpractice because, according to the patient, the physician concealed his negligence. According to the court, this concealment was particularly evident through the physician's letter to the patient's primary care physician detailing the treatment for colitis, yet did not mention the kidney mass.

Statutes of limitations and statutes of repose are complete defenses, even if the physician or care provider's actions were negligent and the patient was injured because of that negligence. The law encourages parties to act rather than sit on their rights. An injured patient must act within the prescribed period — often two to four years — or risk losing their right to file suit. These statutes have nuances, exceptions, and other methods for delaying their application, but it is worthwhile for physicians and care providers to determine their applicability because a successful statute of limitations defense can provide an early defense victory and eliminate the need for trial. ■

REFERENCE

- Decided Oct. 6, 2021, in the Court of Appeals of Iowa, Case Number 20-1124.

Birth Injury Suit Defense Verdict Upheld in Favor of Physician and Practice Group

News: Shoulder dystocia occurred during a delivery, whereby the delivery stalled and risked significant injury to the child. The delivering physician attempted to maneuver the child, but failed to do so properly, and instead negligently injured the child. The defendant care providers raised a state law providing immunity for such simple negligence in emergency situations where a patient is not medically stable.

A jury found in favor of the defendant. The plaintiffs appealed the determination, but the appellate court upheld the verdict.

Background: In 2008, a woman experienced complications while giving birth. During delivery, shoulder dystocia occurred, stalling the process. The delivering physician attempted to maneuver the child, but failed to properly manage the shoulder dystocia. Due to the physician's actions, the child suffered an injury to her brachial plexus nerves.

The child's parents sued the physician and the medical practice group, alleging the physician was grossly negligent during the delivery, and the practice group was liable as his employer. The defendant physician and employer denied wrongdoing or liability, raising various affirmative defenses. Among the affirmative defenses was an applicable state statute that specifically provides physicians immunity from simple negligence in certain malpractice actions. This statute applies only when the malpractice action involved care in an emergency situation with an immediate threat of death or serious bodily injury to the patient receiving care in an emergency department, in an obstetrical suite, or in a surgical suite. Furthermore, the patient must be medically unstable for the statute to apply. If there is no immediate threat of death or serious bodily injury, the statute's protections do not apply.

In this case, the defendant physician claimed this was an emergency situation that presented a medically unstable patient at risk of death or serious bodily injury. The plaintiffs argued the statute did not apply since the patient had a pre-existing doctor/patient relationship, and the statute's language includes different provisions for different circumstances. The plaintiffs sought to eliminate this prospective affirmative defense from the jury's consideration. The trial court agreed with the defendants and determined the section contained two separate and distinct situations, rather than one single defense.

A jury determined that while the physician did negligently harm the child during the delivery, the negligence occurred while the physician was rendering care in an emergency, during which the child was medically unstable and an immediate threat of death or serious bodily harm was present. The specific statutory affirmative defense applied, and the physician was immune from liability. The plaintiffs appealed, arguing the affirmative defense should not have been applied. The plaintiffs did not dispute the factual findings related to the medical circumstances; they admitted shoulder dystocia was a genuine emergency situation, the child was medically unstable, and the circumstances constituted an imminent risk of death or serious bodily injury.

Instead, the plaintiffs attempted to argue the application of these facts to the law and the specifics of the defense, whether it provided for a single defense or separate defenses. The appellate court agreed with the trial court and determined the different subsections provided in the law described different factual scenarios in which a physician would be protected from liability. The appellate court upheld the defense verdict.

What this means to you: This case presents interesting lessons on the facts and the law, in which the former was largely undisputed, and the latter was heavily disputed. On the facts, the child's injury caused by the shoulder dystocia was plainly evident, and the defendants did not argue the brachial plexus nerve injury was not caused by the physician's actions. The injured child and her parents initially argued the physician's actions constituted "gross negligence," an even higher measure of negligence that is more egregious than a standard breach of the duty of care. However, upon the presentation of all the documentary evidence and witness testimony, the child and parents conceded gross negligence did not apply. Each side offers insight into how to reasonably and efficiently proceed in medical malpractice litigation. Conceding on issues that clearly have not been met demonstrates reasonability and can foster goodwill with the court or jury.

Here, both sides surprisingly made material concessions by the defendants' acknowledgment of the patient's injury and by the patient's acknowledgment of the defendants' lack of gross negligence. If either side would have argued, for example, that shoulder dystocia was not a medical emergency, that side certainly would have lost credibility in the eyes of the jury. Shoulder dystocia is a medical emergency that can and does result in brachial plexus injuries, or other significant harm. There are protocols that must be followed to prevent harm to the infant and to expedite delivery, but they can, and often do, result in some sort of injury to the infant's affected arm. If the physician and the staff are following the prescribed procedures correctly, then they are meeting the applicable standards of care, which ideally results in eliminating or reducing injury to the patient as well as protecting from medical malpractice actions. A physician or care provider might take all the right actions, but injury simply is inescapable.

In this case, a specific state law offers more protection for physicians and care providers under limited circumstances — even if the care provider does not adhere to the applicable standards of care. This state law offers immunity from basic or simple negligence when there is a genuine emergency in an emergency department, in an obstetrical suite, or in a surgical suite; when the patient is not medical stable; and when the patient is at imminent risk of death or serious bodily injury. If all three circumstances are satisfied, a negligent physician or care provider will not be liable for medical malpractice. In this matter, the defendants successfully demonstrated all three of the necessary criteria: the shoulder dystocia represented an emergency situation, the child was not medically stable, and the child was at imminent risk of death or serious bodily injury. Because of this, even though the physician failed to act appropriately, the physician could not be held liable as a matter of law.

Lessons from this case on the law may be unique to this state, but it demonstrates the importance of reviewing a physician or care provider's applicable laws for any such special protections. In a different state, the outcome here could have been dramatically different: The physician was negligent and the patient was injured, which could have resulted in a jury awarding millions of dollars for lifelong injuries requiring ongoing medical care. But here, the negligent physician was protected by the state law. Such state-specific protections can be extremely powerful defense tools, eliminating liability altogether (as here), or reducing the extent of liability (by placing a maximum on how much money an injured patient can recover in a medical malpractice action). Care providers should work closely with counsel to understand the nature and scope of any such state-specific protections. ■

REFERENCE

- Decided Oct. 6, 2021, in the Court of Appeals of South Carolina, Case Number 2017-002299.

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

HIPAA Changes Coming in 2022 Might Require Policy Revisions

Proposed changes to HIPAA and HITECH may affect covered entities and business associates in 2022. Now is the time to consider any effects, and respond accordingly.

HHS published proposed modifications to HIPAA and HITECH in early 2021. It appears these changes will be adopted in some form. The modifications could require updates to policies and procedures, notices of privacy practices, forms, business associate agreements, and other HIPAA-related compliance issues. Compliance with some new requirements could be difficult.

(Editor's Note: Read much more about the proposed HIPAA and HITECH modifications online at this link: https://bit.ly/2ZXGld9.)

The proposed modifications to the HIPAA Privacy Rule are intended to improve the coordination of care and to reduce regulatory burden on the healthcare industry, says **Erin Dunlap**, JD, an attorney with Coppersmith Brockelman in Phoenix. While these are important goals in terms of transformation to value-based healthcare, most health plans and covered healthcare providers want to know what the proposed modifications mean for them in the short term from an operational perspective.

"If the proposed modifications are finalized, I think policy work will be front and center for compliance/privacy personnel, followed by appropriate training," Dunlap says. "Patient access will be a key area of focus." Dunlap says finalization of the proposals will mean patient access policies will need to be revised in several ways:

- Require responses to patient access requests within 15 calendar days (vs. the current 30 days) and shorten the possible extension time to 15 calendar days (vs. the current 30 days);
- Prioritize urgent or other high-priority access requests (especially those related to health and safety) and limit the use of an extension for such requests;
- Prohibit "unreasonable" measures that impede individual access to protected health information (PHI), such as requiring an individual to fill out an extensive request form, obtain notarization, or to submit a request in person or only through an online portal;
- Permit a patient to inspect PHI that is readily available at the point of care, such as an X-ray, ultrasound, or lab results;
- Require the electronic transmission of PHI (e.g., by email or through a personal health app, which is defined under the proposed modifications) if the PHI is readily producible through such means;
- Provide access free of charge when a patient inspects PHI in person or uses an internet-based method (e.g., a personal health app);
- Submit a patient's request for an electronic copy of PHI in an electronic health record (EHR) to a covered healthcare provider (i.e., the discloser) within 15 calendar days;
- Allow individuals the right to take notes, videos, and photographs (and other personal resources) to capture PHI in a designated record set, subject to a few limitations.

"While it is unlikely that all of the proposed modifications will be finalized in current form, I think it is important for plans and providers to prepare and budget for significant policy work and training in 2022," Dunlap says.

The proposed changes, if finalized, also will require several revisions to a covered entity's notice of privacy practices (NPP), including changes to the introductory statement and the right of access provision. Organizations

might have to add a statement indicating patients can discuss the notice with a designated contact person and provide such person's email address and phone number. "On a positive note, plans and providers will no longer need to obtain a written acknowledgment or receipt of the NPP," Dunlap says.

More Training Will Be Needed

Most of the proposed changes are intended to improve care coordination and interoperability, says **Eric D. Fader**, JD, partner with Rivkin Radler in New York City. However, the changes would introduce a training burden for covered entities.

"Training of employees has been one of the things that providers have fallen down on in the past 20 years. HIPAA has never been fully complied with by providers because they purchase a HIPAA manual, put it on the shelf, and think they are in compliance," Fader says. "Or, they have employees watch a HIPAA video when they're first onboarded, and that's it. You're really supposed to train and retrain your employees every year at least."

The Office for Civil Rights (OCR) has settled at least 20 Right of Access initiative cases. Fader believes so many settlements indicates covered entities already are struggling to comply with the requirements to allow patient access to records. Now, the proposed changes might introduce even more challenging requirements. *(Editor's Note: Read more about the OCR's 20th settlement, from September 2021, at this link: https://bit.ly/3CMhneY.)*

Fader argues the proposed rules try to change the presumption of HIPAA compliance away from restricting PHI consumption more toward a presumption that data must be shared for care coordination.

"Part of the problem with patients trying to get access to their PHI has been that the organization, or individual employees, would use HIPAA as a crutch, an excuse not to go to the trouble of providing the information," Fader says. "They would say they can't give the patient these data because HIPAA prohibits it, or you have jump through all these hoops before we will give you your own records."

Some covered entities would require excessive written authorizations, sometimes notarized, and they might mandate different requirements for transferring data to certain recipients.

"All of this is going to be changed with these proposed rules if they become effective, which they probably will in virtually the form they are in," Fader offers. "Now, patients are going to have the ability to inspect their PHI in person and take records or photographs. That is potentially a nightmare scenario for some providers, who could have a parade of patients coming in the office to view their records. You'll need to give them a private and secure place to do that, with someone sitting with them to make sure they don't get into things they're not supposed to."

Many states are likely to align their relevant laws with the new HIPAA standards for how long a patient must wait for records. Fader believes some may see OCR's move as a signal to enact even shorter time frames. "In addition to violating HIPAA if you don't get that data to patients in time, you may have to worry about violating state laws as well," he says. "This can all create a burden for covered entities that are not ready for some of the logistical challenges here."

In addition, the proposed rules would allow patients to obtain records in the format they choose. For instance, covered entities might struggle if the electronic record system cannot comply with the format a patient requests.

There also are new definitions of an EHR that includes billing records. If the provider keeps billing records in a separate system, it may have to go into both systems to comply with a request for a full EHR.

Better Care Coordination

Lee Barrett, CEO and executive director of the Electronic Healthcare Network Accreditation Commission (EHNAC) in Simsbury, CT, says his organization supports the HHS objective of removing regulatory obstacles and burdens related to HIPAA. The changes would facilitate efficient care coordination and case management while promoting the transformation to value-based healthcare and preserving the privacy and security of PHI.

"One specific question deals with the requirement for providers to gain a signed copy of the Notice of Privacy Practices. With the implementation of interoperability, this task could easily be handled via a customer portal or secure mobile application," Barrett says. "Likewise, there are questions about whether or not non-HIPAA-covered entities should participate in data exchange. The current movement toward electronic healthcare data exchange allows for non-HIPAA-covered entities to contribute, but only after identity is validated and

their feedback can be obtained in a secured fashion."

EHNAC has worked with organizations like the Workgroup for Electronic Data Interchange and others to facilitate the industry's implementation of HIPAA Privacy and Security requirements. "While minor adjustments to the regulations could lessen some burdens on some organizations, the full focus of our collective energy and efforts should be on driving industry adoption of standards associated with the secure and efficient exchange of health information in an interoperable manner," Barrett says. "Once our industry attains a high adoption percentage demonstrating interoperability, many of the current issues experienced as challenges with the rules will be significantly lessened."

The pending HIPAA changes are mostly an attempt to encode pre-existing subregulatory guidance or best practices, according to **Matt Fisher**, JD, general counsel for Carium, a telehealth and remote patient monitoring company based in Petaluma, CA

"With that in mind, organizations should prepare to boost efforts related to access by individuals and care coordination. Arguably both of those areas should already be receiving attention, given recent enforcement actions by the Office for Civil Rights and the aims of value-based care or population health initiatives," Fisher says. "That all means the pending changes should be seen as another kick to implement procedures that should already be in place." ■

SOURCES

- **Lee Barrett**, CEO and Executive Director, Electronic Healthcare Network Accreditation Commission, Simsbury, CT. Phone: (860) 408-1620.
- **Erin Dunlap**, JD, Coppersmith Brockelman, Phoenix. Phone: (314) 255-5988. Email: edunlap@cblawyers.com.
- **Eric D. Fader**, JD, Partner, Rivkin Radler, New York City. Phone: (212) 455-9570. Email: eric.fader@rivkin.com.
- **Matt Fisher**, JD, General Counsel, Carium, Petaluma, CA. Phone: (508) 603-9202. Email: matt.fisher@carium.com.

HIPAA Relevance to COVID-19 Vaccinations Can Be Misunderstood

Employees and employers frequently believe HIPAA comes into play when asking about an individual's vaccination status. It almost always does not, according to **Carly O. Machasic**, JD, attorney with Clark Hill in Detroit.

Although some states are considering legislation designating vaccination status as a separate protected class, private employers generally are free to ask employees about their vaccination status without running afoul of HIPAA or federal employment laws. HHS guidance released earlier this year points out the HIPAA Privacy Rule regulates "how" and "when" certain entities covered by HIPAA are permitted to "use and disclose" an employee's health information, not whether they can "request" it. The HHS guidance was intended "to help consumers, businesses, and healthcare entities understand when HIPAA applies to disclosures about COVID-19 vaccination status" and related issues. *(Editor's Note: The HHS guidance is available online at this link: https://bit.ly/3mHic36.)*

A recurring theme throughout the pandemic is the surplus of misinformation, and the relationship between HIPAA and one's COVID-19 vaccination status is no exception, says **Stuart F. Miller**, JD, shareholder with Munsch Hardt in Houston. As employers and places of business have begun asking employees and customers about their vaccination status, many claim HIPAA protects their personal vaccination information, arguing they are not required to disclose their vaccination status. Others claim the employees would be violating HIPAA by disclosing their vaccination history.

Miller believes the HHS guidance proves these claims are false. The HIPAA Privacy Rule applies to covered entities, such as healthcare providers, and (to a certain extent) their business associates. The rule is not about if covered entities can ask for this information; it regulates how that information is shared and stored.

"Generally, the privacy rule does not regulate what information can be requested from employees as part of the terms and conditions of employment that an employer may impose on its workforce. However, other federal or state laws do address terms and conditions of employment," HHS explained in its guidance. "For example, federal antidiscrimination laws do not prevent an employer from choosing

to require that all employees physically entering the workplace be vaccinated against COVID-19 and provide documentation or other confirmation that they have met this requirement, subject to reasonable accommodation provisions and other equal employment opportunity considerations. Documentation or other confirmation of vaccination, however, must be kept confidential and stored separately from the employee's personnel files under Title I of the Americans with Disabilities Act."

According to the HHS guidance, HIPAA does not prohibit a covered entity or business associate from requiring or requesting each employee to:

- Provide documentation of their COVID-19 or flu vaccination to their current or prospective employer.
- Sign a HIPAA authorization for a covered healthcare provider to disclose the employee's COVID-19 vaccination record to their employer.
- Wear a mask while in the employer's facility, on the employer's property, or in the normal course of performing their duties at another location.
- Disclose whether they have received a COVID-19 vaccine in response to queries from current or prospective patients.

The privacy rule forbids covered entities from disclosing anyone's protected health information (PHI), which includes vaccination status, without that person's authorization. As HHS defines it, disclosing PHI "is limited to information that is reasonably necessary to accomplish the stated purpose of the disclosure." The agency offers some examples of permitted PHI disclosures that are relevant to this issue:

- A covered physician is permitted to disclose PHI regarding a vaccination to an individual's health plan to obtain payment for the administration of a COVID-19 vaccine.
- A covered pharmacy is permitted to disclose PHI relating to an individual's vaccination status to a public health authority.
- A health plan is permitted to disclose an individual's vaccination status when required to do so by law.
- A covered nurse practitioner is permitted to provide PHI relating to an individual's COVID-19 vaccination status to the individual.

"A covered hospital is permitted to disclose PHI relating to an individual's vaccination status to the individual's employer so that the employer may conduct an evaluation relating to medical surveillance of the workplace (e.g., surveillance of the spread of COVID-19 within the workforce) or to evaluate whether the individual has a work-related illness," HHS explained in its guidance. However, according to the agency, these conditions have to be met:

- The covered hospital is providing the service to the individual at the request of his or her employer or as a member of the employer's workforce.
- The disclosed PHI consists of findings concerning work-related illness or workplace-related medical surveillance.
- The employer needs the findings to comply with the Occupational Safety and Health Administration or state laws with a similar purpose.
- The covered healthcare provider provides written notice to the individual that the PHI related to the medical surveillance of the workplace and work-related illnesses will be disclosed to the employer. ■