HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE FOR MORE THAN THREE DECADES

INSIDE

AHC Media
A RELIAS LEARNING COMPANY

SEPTEMBER 2017 Vol. 39, No. 9; p. 97-108

Medicare Fraud Bust Sends Warning to Healthcare Providers

412 charged in biggest operation ever by Medicare strike force

The huge federal crackdown on Medicare fraud opioid abuse is a loud alarm bell for risk managers in all healthcare settings, signaling that the Department of Health and Human Services (HHS) and the Department of Justice (DOJ) are not fooling around. They're charging people by the hundreds, and for the first time a large proportion are healthcare professionals.

Hundreds also are excluded from Medicare participation, essentially a death sentence for their careers in medicine.

The largest-ever healthcare fraud enforcement action by the Medicare Fraud Strike Force involved 412 defendants across 41 federal districts, including 115 doctors, nurses, and other licensed medical professionals, all charged for their alleged participation in healthcare fraud schemes involving approximately $1.3 billion in false billings.

> THE LARGEST EVER HEALTHCARE FRAUD ENFORCEMENT ACTION BY THE MEDICARE FRAUD STRIKE FORCE INVOLVED 412 CHARGED DEFENDANTS ACROSS 41 FEDERAL DISTRICTS.

Of those charged, more than 120 defendants, including doctors, were charged for their roles in prescribing and distributing opioids and other dangerous narcotics.

HHS Secretary **Tom Price**, MD, announced the action recently. Thirty state Medicaid Fraud Control Units also participated in the arrests. In addition, HHS has initiated suspension actions

Financial Disclosure: Author **Greg Freeman**, Editor **Jill Drachenberg**, Editor **Jonathan Springston**, AHC Media Editorial Group Manager **Terrey L. Hatcher,** Nurse Planner **Maureen Archambault,** and Guest Columnist **Joseph M. Gorrell, JD,** report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study. Physician Editor **Arnold Mackles**, MD, MBA, LHRM, discloses that he is an author and advisory board member for The Sullivan Group and that he is owner, stockholder, presenter, author, and consultant for Innovative Healthcare Compliance Group.

HEALTHCARE RISK MANAGEMENT™

Healthcare Risk Management™,
ISSN 1081-6534, including *Legal Review & Commentary*™
is published monthly by
AHC Media, LLC, a Relias Learning company
111 Corning Road, Suite 250
Cary, NC 27518

Periodicals Postage Paid at Atlanta, GA 30304 and at additional mailing offices
GST Registration Number: R128870672

POSTMASTER: Send address changes to: *Healthcare Risk Management*
P.O. Box 74008694
Chicago, IL 60674-8694

SUBSCRIBER INFORMATION: Customer Service: (800) 688-2421. Customer.Service@AHCMedia.com
AHCMedia.com

SUBSCRIPTION PRICES: USA, Print: 1 year (12 issues) with free CE nursing contact hours and free *AMA PRA Category 1 Credits*™, $519. Add $19.99 for shipping & handling. Online only, single user: 1 year with free CE nursing contact hours and free AMA PRA Category 1 Credits™, $469. Outside USA, add $30 per year, total prepaid in USA funds.

MULTIPLE COPIES: Discounts are available for group subscriptions, multiple copies, site-licenses, or electronic distribution. For pricing information, please contact our Group Account Managers at Groups@AHCMedia.com or (866) 213-0844. Missing issues will be fulfilled by customer service free of charge when contacted within one month of the missing issue date. Back issues, when available, are $87 each. (GST registration number R128870672.)

ACCREDITATION: Relias Learning, LLC, is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation. Contact hours [1.5] will be awarded to participants who meet the criteria for successful completion. California Board of Registered Nursing, Provider CEP#13791.

Relias Learning is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians. Relias Learning 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 an activity.

Healthcare Risk Management™ is intended for risk managers, healthcare administrators, healthcare legal counsel, and physicians. This activity is valid 36 months from the date of publication.

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
AHC MEDIA EDITORIAL GROUP MANAGER: Terrey L. Hatcher
SENIOR ACCREDITATIONS OFFICER: Lee Landenberger

EDITORIAL QUESTIONS
Call Editor **Jill Drachenberg**, (404) 262-5508

against 295 providers, including doctors, nurses, and pharmacists.

"The charges announced today aggressively target schemes billing Medicare, Medicaid, and TRICARE [a health insurance program for members and veterans of the armed forces and their families] for medically unnecessary prescription drugs and compounded medications that often were never even purchased and/or distributed to beneficiaries," HHS stated in an announcement of the charges. "The charges also involve individuals contributing to the opioid epidemic, with a particular focus on medical professionals involved in the unlawful distribution of opioids and other prescription narcotics, a particular focus for the department. According to the CDC, approximately 91 Americans die every day of an opioid-related overdose."

Kickbacks, Fraudulent Billing

According to court documents, the defendants allegedly participated in schemes to submit claims to Medicare, Medicaid, and TRICARE for treatments that were medically unnecessary and often never provided. In many cases, patient recruiters, beneficiaries, and other co-conspirators allegedly were paid cash kickbacks in return for supplying beneficiary information to providers, so that the providers could then submit fraudulent bills to Medicare for services that were medically unnecessary or never performed.

The number of medical professionals charged is particularly significant, HHS said, "because virtually every healthcare fraud scheme requires a corrupt medical professional to be involved in order for Medicare or Medicaid to pay the fraudulent claims." Aggressively pursuing corrupt medical professionals not only deters other medical professionals, but also ensures that their licenses can no longer be used to bilk the system, HHS added.

OIG, HHS, and the FBI all pledged to continue vigorously pursuing those who abuse federal healthcare programs.

'Enormous' Case Took Years

The scope of the legal action is noteworthy, says **Kenneth Yeadon**, JD, a former assistant U.S. attorney with the U.S. Attorney's Office in Chicago and now a partner at Hinshaw & Culbertson in

EXECUTIVE SUMMARY

Federal officials recently charged 412 people across the country with healthcare fraud related to false billings, and many were healthcare professionals. A substantial portion of the charges relate to the fraudulent prescription of opioids.

- More people may be charged.
- The crackdown shows the need to follow opioid prescribing guidelines.
- Hospitals and health systems should audit Medicare billings more closely than ever.

Chicago. In his time with the U.S. Attorney's Office in Chicago, he led several significant investigations and prosecutions, including those involving healthcare and tax fraud, and money laundering.

"This is an enormous healthcare fraud case that likely took years to put together. Nearly one-half of the country's federal prosecutors' offices — U.S. Attorney's offices — were involved," he says. "In addition to its massive scale, one of the things that makes this action unique is the focus on healthcare professionals. More than 100 doctors, nurses, and healthcare professionals are being prosecuted for illegally distributing opioids and other prescription narcotics, and healthcare fraud."

However, even with such a large scope there could be more arrests and charges, he says.

"Healthcare providers can expect this case to mushroom exponentially as people who have been charged begin to talk, leading to the likelihood that many more will be charged," Yeadon says. "With so many healthcare agencies, law enforcement officials, and even the IRS involved, the charges against healthcare providers are likely to be wide-ranging. In addition to fraudulent billing, they may include money laundering and tax fraud."

The government is sending a clear message with the arrests, says **Jesse Witten**, JD, partner with the law firm Drinker Biddle in Washington, DC. Officials didn't have to round up everyone at once and make such

DOJ Launches Opioid Fraud Unit With Big Data

Soon after its largest-ever bust of healthcare providers involved in the fraudulent distribution of opioids, the Department of Justice announced a new Opioid Fraud and Abuse Detection Unit that draws on healthcare data analytics to find misuse of controlled substances.

The task force will focus specifically on slashing fraud originating in the healthcare system, with 12 prosecutors overseeing the following regions that have been hit hard by the ongoing opioid epidemic:

1. Middle District of Florida,
2. Eastern District of Michigan,
3. Northern District of Alabama,
4. Eastern District of Tennessee,
5. District of Nevada,
6. Eastern District of Kentucky,
7. District of Maryland,
8. Western District of Pennsylvania,
9. Southern District of Ohio,
10. Eastern District of California,
11. Middle District of North Carolina,
12. Southern District of West Virginia.

U.S. Attorney General **Jeff Sessions** announced the formation of the new unit, noting that opioid overdoses and related health problems took the lives of close to 60,000 Americans last year.

"I am announcing a new data analytics program — the Opioid Fraud and Abuse Detection Unit," Sessions said in a statement. "I have created this unit to focus specifically on opioid-related healthcare fraud using data to identify and prosecute individuals that are contributing to this opioid epidemic. This sort of data analytics team can tell us important information about prescription opioids — like which physicians are writing opioid prescriptions at a rate that far exceeds their peers; how many of a doctor's patients died within 60 days of an opioid prescription; the average age of the patients receiving these prescriptions; pharmacies that are dispensing disproportionately large amounts of opioids; and regional hot spots for opioid issues."

Even though every state has an electronic prescription drug tracking system, Sessions said collecting and using opioid-related data to reduce overdoses, limit access, and prevent addiction continues to be difficult due to data silos and jurisdiction limits, combined with poor interoperability and fragmented data collection. ■

a show of the operation, he says, but they acted with a purpose.

"They filed all these charges and announced all the exclusion actions on a single day to make as big a splash as they could, rather than spread them out over a period of time," Witten says. "The idea of a mass takedown is not new because they do it every year, but it's much bigger in terms of the number of people being pursued."

Officials widened the scope of their investigation to include opioid distribution and more healthcare professionals than in previous years, he says. The number of exclusions also is significant, he says.

"Criminal charges are serious, of course, but the 295 individuals being excluded are over and above the 412 being criminally charged, so we're talking about over 700 people," he says. "That's very resource-intensive for the OIG, so they're sending the message that they are making Medicare fraud, and the opioid issue in particular, a top concern."

It is not yet clear how the OIG investigated the individuals and reached decisions to charge and exclude them, Witten notes. The government may have relied on prescribing records and other data, but it is possible that the investigation involved whistleblowers and other direct information from those with knowledge of the crimes.

"I speculate that a lot of the nurses are being pursued because of drug diversion. This is an increasingly difficult issue for hospitals with employees of all types, but especially for nurses because they usually have access to the drugs," Witten says. "Clamping down on controlled drugs, and opioids in particular, is not a new idea for healthcare organizations, but this brings attention to the fact that the government is going to be bringing enforcement actions that are far-reaching and which have very serious consequences."

In addition to fraud and exclusion risks, Witten points out that hospitals face liability risks from threats to patient safety related to drug diversion. If patients do not receive proper medication because it was diverted by an employee or physician, the hospital can be held liable for the consequences. The same applies if a patient is harmed by an impaired healthcare provider.

> "IF ANYONE IN THE ORGANIZATION WAS DOUBTING THE SERIOUSNESS OF THIS PROBLEM AND JUST HOW SERIOUSLY THE GOVERNMENT IS TAKING THIS, YOU SHOULD HAVE A GOOD WAY TO DISPEL THOSE OBJECTIONS. NOW IS THE TIME TO PROTECT YOURSELF."

"There's still room there for action by Medicare and the Department of Justice, but the bigger issue there would be the opportunity for some sort of malpractice action," Witten says. "If you're a patient who's only getting half the pain medication you're supposed to get because somebody is diverting the other half, those patients will not be happy when they come to learn about that. I wouldn't be surprised if plaintiffs' attorneys in those areas are on high alert for those cases now."

Risk managers at hospitals and health systems should work with the internal compliance or audit departments, and the pharmacy department, to review internal controls intended to protect controlled substance dispensing, he says.

"This would also be a good reason to conduct an audit of controlled substances and dispensing activities to look for any signs of suspicious patterns or activity," Witten says. "If anyone in the organization was doubting the seriousness of this problem and just how seriously the government is taking this, you should have a good way to dispel those objections. Now is the time to protect yourself."

Yeadon agrees that the massive takedown represents a good opportunity for action. *(See the story on page 99 about a new DOJ initiative to use big data analytics to identify opioid fraud, and the story on page 101 for advice on how to avoid liability with opioids.)*

"Healthcare providers should not wait for this case to envelop them," Yeadon says. "They should begin taking immediate action to focus on Medicare/Medicaid billings in anticipation of tighter controls over payments on claims and increased audits." ■

SOURCES

- **Jesse Witten**, JD, Partner, Drinker Biddle, Washington, DC. Phone: (202) 230-5146. Email: jesse.witten@dbr.com.
- **Kenneth Yeadon**, JD, Partner, Hinshaw & Culbertson, Chicago. Phone: (312) 704-3524. Email: kyeadon@hinshawlaw.com.

Prescribing Opioids: Physicians Must Assess Carefully, Document Rigorously to Avoid Liability

By Joseph M. Gorrell, JD
Healthcare Law Attorney, Brach Eichler
Roseland, NJ

The human toll of the opioid crisis is enormous, with millions of Americans suffering from addiction and more than 90 people dying each day from opioid overdoses. It is widely recognized that a significant part of the problem is the overprescription of pain medications, such as oxycodone and fentanyl. For physicians who prescribe such medications, this presents important challenges.

Physicians must weigh carefully the benefit that such medications can provide to a given patient in severe pain while meticulously documenting their actions in compliance with increased regulatory oversight. In a worst-case scenario, failure to do either could lead to sanctions against a physician's license.

In meeting these challenges, there is an increased need for physicians to ensure that they thoroughly examine their patients and rigorously document the care they are providing. Accepted standards of medical practice demand that physicians enter contemporaneous notes in the medical record containing the patient's complaints, history, findings on appropriate examination, orders for tests or consultations, and diagnosis or medical impression.

When prescriptions are written, they must be preceded by an examination or evaluation of the patient, as appropriate, and the name, strength, and quantity of the medication should be contained, not only on the prescription, but in the medical record, either by placing a copy of the prescription in the chart or by documenting the necessary information in the progress note.

Concurrently, the increased use of electronic medical records (EMRs) presents the need for physicians to be vigilant about the reliability and maintenance of their EMR system. In my representation of pain management physicians, two examples have arisen recently that illustrate these points.

In one case, a physician who worked in a three-physician practice suddenly was faced with an owner of the practice who abruptly retired, and another who suffered a medical emergency that led to a six-month disability. The physician was alone in his practice and, unfortunately, the EMR system was not functioning properly. He had spent his entire career using paper records, and he did not have a firm grasp of how to use the EMR system. Furthermore, because he was not an owner of the practice, he did not have the authority to invest the practice's money in fixing the system.

The result? Critical information gathered by the physician — patient histories, notes from examinations, and prescriptions written — did not become part of the patients' medical record. Because his patient population consisted primarily of patients who required pain management, and because he prescribed a significant amount of opioids to manage his patients' pain, his practice came under the scrutiny of the state licensing authority.

As a consequence, several of the physician's patient records were subpoenaed by the licensing authority. When he reviewed those records prior to turning them over, the physician was mortified to see the wide gaps in his medical record.

Thus, even though he obtained a complete history and conducted a thorough examination of each of his patients on each visit, documentation was lacking. When he was called before an investigating committee of that licensing authority, the members were less than pleased.

In a second, similar case, the physician, who also practiced pain management and prescribed a significant amount of opioids for patients who were in severe pain, was in the process of converting his EMR system from one vendor to another. He also drew the attention of the state licensing authority due to the amount of opioids he was prescribing. When his medical records were subpoenaed, he was unable to produce the complete charts because, in the transition, the substance of many of his progress notes, as well as other components of the medical record, had disappeared.

The result has been devastating. In part, because of these missing records as well as other factors, the physician's license has been temporarily suspended pending a full hearing.

How can physicians avoid such calamitous results? Physicians must understand that they will be held responsible for breakdowns in documentation that occur in their

offices. The buck stops with the physicians providing the care. It is not the IT vendor who installs a faulty system that will pay the price for an inoperable EMR system — it is the physician. It is incumbent on physicians who use an EMR to ensure it is operating properly and that they know how to use it. This requires ongoing monitoring of the EMR system and immediate remedial action if problems arise. Waiting is not an option.

Furthermore, physicians using an EMR should internally monitor their records to assure themselves that the system is working properly and, equally important, that they are using it appropriately. When physicians see a patient, they need only check their previous progress note to confirm that their documentation of the previous visit was entered into the record properly.

Physicians also should scrutinize and become familiar with regulations promulgated by their state licensing authority so they can ensure that they are complying with requirements for prescribing, particularly when controlled, dangerous substances are involved.

These regulations will likely specify:

1. appropriate dosage, strength, and quantity of the medication;
2. under what circumstances multiple prescriptions may be written;
3. whether a specific treatment plan must be developed;
4. whether the physician must access a state prescription monitoring program;
5. the necessity of a thorough medical history, including the nature, frequency, and severity of pain.

In today's regulatory environment, it is highly recommended that physicians conduct audits of their medical records and billing procedures to ensure that their billing practices also are appropriate.

The current opioid crisis highlights how important it is for physicians to make concerted efforts to thoroughly document the details of their encounters with their patients and to ensure that their EMR systems are functioning properly by way of ongoing monitoring and periodic audits. With state licensing authorities putting the spotlight on those who don't comply — and, in some cases, imposing strict sanctions — physicians cannot afford to be complacent. ■

SOURCE

- **Joseph M. Gorrell**, JD, Brach Eichler, Roseland, NJ. Telephone: (973) 403-3112. Email: jgorrell@bracheichler.com.

Health System Cuts Workers' Comp With Best Docs

Health systems can significantly reduce their workers' compensation expenses by identifying and using high-performing physicians in medical networks, according to the experience of operators of one system in California, which saw overall claims costs reduced by almost 20%.

The premise of the program is that if one begins with treatment rendered by top-performing physicians who have demonstrated better outcomes, he or she will enhance the overall outcome of the entire book of business, says **Linda Lane**, president of Harbor Health Systems in Newport Beach, CA.

"Over time, that can lead to a significant impact with both a reduction in total medical spend and in total indemnity," she says. "It's a program that takes advantage of data analytics and allows our risk managers and payer partners to utilize what they may already have in place."

Harbor Health Systems identified the highest-performing physicians and directed injured patients to them. Harbor manages or owns 154 medical provider networks (MPNs) nationwide, with 1.7 million patients enrolled. The company developed a proprietary software suite, MD 360, that examines 20 different variables within the MPNs treating workers' compensation claimants.

Algorithms Identify Top Docs

The effort began in 2001 when the company founder's physician wife was frustrated at the inability to promote her better outcomes with treating workers' comp cases, Lane explains. MPNs seek to be broad and deep, but in past years they have not focused enough on outcomes data to allow one doctor's results to stand out.

In response, Harbor Health asked a group of biostatisticians to create a proprietary set of algorithms that look at 20 points from three sets of data: claims data from a payer,

network data to identify the treating physicians, and billing data to identify the treatment and billing patterns from those physicians.

"We mine those three data sources and run them through the algorithms to assess impact on permanent total disability days, total medical, litigation, and a number of other criteria," she says. "The model allows us to assess one particular provider in a specialty, and the outcomes associated with that provider, in comparison to his or her peer group. We're looking at a specialist in one geographic area compared to peers in that same area."

Harbor Health does not evaluate medical skills of individual physicians, but uses a scoring method based on a retrospective analysis of closed claims, Lane explains. Among the criteria examined are cost of treatment, duration of treatment, patient recidivism, and litigation involving the claim. All the measures are objective, rather than including any subjective measure of medical performance.

"The elements that we use really rely on data being clean, and in our industry when you talk about billing and network data, that's one of the biggest challenges," Lane says. "Wrapped around our model is also a very stringent identity management piece, which is crucial to identifying that single individual doctor or that unique group. If you can't do that, you can't apply the measures."

Not Easy to Compile Data

One challenge is accurately identifying physicians so one can associate their outcomes data. It is common for there to be a PPO network, but also other provider networks to ensure accessibility wherever a covered claim might exist, Lane notes. A particular doctor might be a member of one's primary network, but also several others. In each of those networks, the same physician may be listed differently: John Smith, John A. Smith, J. Smith, J.A. Smith, J. Smith-Jones, etc. The same physician also may list multiple addresses and multiple associations with treatment groups.

"Getting down to that individual doctor and being able to collapse all the information about that individual into one set of data is the first critical piece of our work," she says. "We've overcome that with some processes that cleanse that data to get to what we call a golden record, which allows us to know we're talking about the same person no matter where data originates. You have to do the same thing with billing, which is just as challenging."

The scoring model has continued to evolve, and recently Harbor Health began to factor in case mix — large loss claims vs. bumps and bruises. This accounts for the fact that some physicians treat only serious injuries, which can skew their outcomes data. Comorbidities such as diabetes and obesity also are considered.

Claims Costs Cut 20%

The goal is to assess the likelihood that a particular spine surgeon in one community will produce as good, better, or worse an outcome with a patient than other spine surgeons Harbor Health could choose instead. Then, clients use Harbor's software suite to schedule patients for the higher-scoring physicians, and to manage and measure the outcomes.

The program also focuses on helping workers' comp patients stay on track with treatment, Lane notes.

Harbor has cut overall claims costs by nearly 20% and indemnity-related costs by nearly one-third, compared to some other workers' compensation management firms. In one instance in which a third-party administrator used Harbor Health's platforms, closed claims increased by 50% and the average claim amount dropped by 9.1% within nine months.

"This is a direct result of not allowing patients to go to any physician in a broad network, and instead directing them to top-performing physicians," Lane says. "You can effect change in these categories just by highlighting and utilizing those good habits that those top-performing physicians innately have." ■

EXECUTIVE SUMMARY

A California health system has cut workers' comp costs by concentrating on using the physicians with the best treatment results. The program examines 20 different variables.

- Overall claims costs dropped almost 20%.
- Indemnity-related costs dropped by nearly one-third.
- Cost of treatment is only one variable considered.

SOURCE

- **Linda Lane**, President, Harbor Health Systems, Newport Beach, CA. Telephone: (949) 536-7068.

OR Fire Safety Improving With More Drills, Less Alcohol Prep

Hospitals are taking fire safety in the OR seriously but still must conduct frequent reviews and update policies as necessary, says **Solveig Dittmann**, RN, BA, BSN, CPHRM, senior risk specialist with Coverys, a medical professional liability insurer in Boston.

Dittmann frequently visits hospitals to assess risk management issues such as OR fire safety and sees more hospitals conducting OR fire drills on a regular basis, at least annually and some even quarterly. That is an improvement over recent years, she says.

"Not everyone is doing the drills or even the surgical fire safety education, but the numbers are increasing dramatically," Dittmann says. "There have been incidents in the news that got attention, including one in which a premature baby was having surgery and there was a fire that ended up injuring her quite severely. There was also a 30-year Chicago firefighter who had never been burned on duty, but suffered severe facial burns during a stent placement."

At a recent hospital perioperative assessment, Dittmann learned there had been no perioperative fire incident for about 30 years, and only a month before her visit had begun conducting OR fire drills with all staff. A week after everyone had been trained, the first OR fire occurred.

"They told me almost tearfully that had they not had that drill, they hated to think what would have happened to the patient," she says. "But because they had the drills, they managed to control the fire so quickly that the patient wasn't harmed at all. It really speaks to the importance of the drills."

> "THEY TOLD ME ALMOST TEARFULLY THAT HAD THEY NOT HAD THAT DRILL, THEY HATED TO THINK WHAT WOULD HAVE HAPPENED TO THE PATIENT."

She also notices that more perioperative teams are including a fire risk assessment as part of their timeout protocol. That was not the case even a few years ago, she says.

"They're asking questions like whether they really need to use 100% oxygen if they're using cautery or laser around the face, neck, or upper torso. That's the biggest risk for an airway fire," she says. "More teams are consistently doing that, and that's a very good change."

More hospitals also are eliminating alcohol-based prep solutions, she says, favoring less flammable options like Betadine. Those sticking with alcohol-based preps take extra precautions, such as making sure the alcohol dries thoroughly before applying drapes, so the drapes don't become saturated and more flammable.

Another development involves notification technology for OR fires, says **Thomas Connell**, senior product manager for Johnson Controls in Westminster, MA. Previous fire alarm technology was broad and signaled a general fire alarm in a part of the hospital or a particular department, but newer technology allows for directed alarms and limited evacuations, he says.

"This can be important in a healthcare setting where you don't want to interrupt procedures going on in the entire surgery center or department, in cases where it is not necessary to evacuate the entire facility," Connell explains. "You can send directed alarms and notifications to only certain areas or certain individuals telling them what the situation is and what to do, rather than sounding a general alarm and leaving it up to individuals to decide based on surroundings and visual clues what they should do." ■

EXECUTIVE SUMMARY

Fire safety in the surgical suite requires frequent review and assessment. Hospitals are paying more attention to the issue, improving policies and procedures.

- More hospitals are conducting OR fire drills.
- Hospitals also are including OR fire safety in surgical timeouts.
- Alcohol-based prep solutions have been eliminated in some facilities.

SOURCES

- Solveig Dittmann, RN, BA, BSN, CPHRM, Senior Risk Specialist, Coverys, Boston. Phone: (517) 866-7999. Email: sdittmann@coverys.com.
- Thomas Connell, Senior Product Manager, Johnson Controls, Westminster, MA. Phone: (888) 746-7539.

Factor Consumerism Into Risk Management

Consumerism is a growing force in healthcare and should be incorporated into a hospital or health system's risk management strategy, says **Jane Harper**, CISSP, CRISC, CRCMP, ISA, PCIP, CISA, ITIL, director of privacy and security risk manager at Henry Ford Health System in Detroit.

Healthcare consumers increasingly are interested and involved in choosing their care, wanting more information and transparency than ever before. This consumerism is changing how healthcare is provided, and risk managers must respond along with other healthcare leaders, says Harper, whose background is in enterprise risk management with a focus on operational risk.

The changing involvement of consumers affects how risk is assessed and managed, she says. Risk managers may need to expand the idea of what risks face the organization, she suggests.

"Twenty years ago, the health insurance plan you got was whatever your employer offered, but in this new world of healthcare consumerism, individuals are able to go out and pick their own plans, elect to have higher deductibles, and control more of the payment between them, the payer, and the healthcare provider," she says.

"That now expands your risk scope beyond just the traditional electronic protected health information [ePHI] assessment, malpractice insurance, and cyberinsurance. It expands to some risks that not everyone is identifying and managing yet."

> "WE HAVE TO GET AWAY FROM THE IDEA THAT WHEN WE TALK ABOUT RISK MANAGEMENT, WE'RE ONLY CONCERNED WITH MALPRACTICE INSURANCE, EPHI, PATIENT SAFETY."

For instance, higher deductibles may lead more healthcare providers to set up credit plans. That creates a credit risk, Harper notes. Reimbursement also can be affected by consumer expectations and ratings, but Harper says few organizations are considering and addressing that risk.

With hospitals increasingly receiving direct payments from patients rather than from insurers, there are concerns such as complying with the Payment Card Industry Data Security Standard (PCI DSS), an information security standard for organizations that handle branded credit cards from the major card companies. There are similar standards for accepting checks or accepting bank transfers, Harper notes.

"We have to get away from the idea that when we talk about risk management, we're only concerned with malpractice insurance, ePHI, patient safety. Those are essential and important concerns, of course, but they're not the only risks facing healthcare organizations today," Harper says. "Consumerism is forcing us to look at a wider scope of risks."

An expanded risk management program that accounts for consumerism should include a wide array of stakeholders, Harper says. That means not just the clinical side, but the other organizational areas influenced by consumerism, such as revenue and reimbursement. Then, an important step is gauging the organization's risk appetite and tolerance, Harper says.

"You can't do just one. You have to determine both the risk appetite and the tolerance for risk to be effective," she says. "That sometimes can be intimidating to certain leaders because your key stakeholders you want to include in an enterprise risk management program won't always have a detailed understanding of risk. They don't necessarily have to, and we shouldn't let that frighten them away from participating."

The risk manager and other experts who run the program can provide the education needed to make the key leaders comfortable in participating, she says.

EXECUTIVE SUMMARY

Consumers increasingly are involved in healthcare payments and demand transparency. This consumerism should be incorporated into risk management programs.

- Direct payment from patients introduces new risks for healthcare organizations.
- Risk managers should consider expanding the scope of risk concerns.
- Fully assessing consumerism impact can help prioritize resources.

Identify Risk Tolerance, Appetite

Once key leaders are on board, there must be a structure to identify what issues matter most to the organization, and the corresponding risk tolerance and appetite for each, she says. At Henry Ford, any identified risks are assessed for the effect they could have on more than just one category. For example, the risk may have operational impact, market impact, or credit impact.

"It gives you the full weight of the issue. We know that every organization has a budget and a set number of resources, so this allows us to prioritize how we manage risks," Harper says. "We might determine that this risk affects us significantly in five different areas, whereas this other risk is important but affects us in only one area. If we have this amount of money and time, putting them next to each other like that helps us prioritize what work gets done and when."

For instance, a few years ago Henry Ford considered the purchase of a governance, risk management, and compliance (GRC) tool and assessed the potential related risks. Harper and other leaders determined that not using a GRC tool meant important issues could be missed, inappropriately prioritized, or receive too much funding that could have been better spent.

"It showed us that we had issues that could affect us in many parts of our operational space — compliance risk, legal risk, making sure we're doing reviews of our data center, many other areas. It ended up affecting four major categories and seven or eight subcategories, so naturally that rose to the top of the list of priorities," she says. "That helped us champion with the senior leadership the purchase of a centralized GRC tool."

Understanding and responding to consumerism can be the key to surviving the uncertain future of healthcare, Harper says. Risk managers are well advised to make themselves the organization's experts on consumerism and incorporate the philosophy into their work, she says.

"I firmly believe that the organizations that are able to identify, quantify, and manage their risks will be the ones that emerge victorious in this era of increased consumerism," Harper says. ■

SOURCE

- Jane Harper, CISSP, CRISC, CRCMP, ISA, PCIP, CISA, ITIL, Director of Privacy and Security Risk Manager, Henry Ford Health System, Detroit. Phone: (800) 436-7936.

Lawyer Reprimanded for Penis Amputation Lawsuit

A lawyer who represented a client in a case that gained national media attention has been reprimanded by the court for not reviewing medical records to determine if his client's case was viable.

John Patrick Graves, JD, in Irondale, AL, represented a man who filed a medical malpractice lawsuit against three physicians in 2014, contending they partially amputated his penis during what was to be a routine circumcision.

A Jefferson County judge dismissed the suit in August 2014, saying it did not meet the higher pleading requirements of the Alabama Medical Liability Act, but allowed Graves to file an amended suit.

Recently, the Alabama Board of Bar Commissioners ordered Graves receive a public reprimand for violating an Alabama rule of criminal procedure, according to a disciplinary notice in *The Alabama Lawyer*, a state bar publication.

The notice said the attorney should have known that at least some of the claims against the physicians were false. Graves had access to and should have reviewed medical records and information that "demonstrated initial claims and allegations against one or more doctors were clearly improper," the notice said. The amended complaint included "plainly false allegations" and included defendants who should not have been sued, according to the notice.

The amended suit contained claims and maintained allegations "that were clearly without merit," the notice said. Graves knew or should have known the meritless claims in the amended complaint "served no purpose other than to harass or maliciously injure one or more defendants," the notice said.

In their response to the lawsuit, the physicians said they did not amputate any portion of the penis when they performed a circumcision for medical reasons, but there was dead tissue after the circumcision because of circulation issues, caused partly by uncontrolled diabetes. ■

Carolina Healthcare System to Pay $6.5 Million for False Claims

Carolinas Healthcare System (CHS) has agreed to pay the federal government $6.5 million to resolve allegations that the company violated the False Claims Act by up-coding claims for urine drug tests to receive higher payment than allowed for the tests.

According to court documents, from 2011 to 2015, CHS conducted "moderate complexity" tests, but submitted claims that indicated the company had conducted "high complexity" tests.

The government alleged that CHS engaged in up-coding by submitting claims using code G0431, which should be used only for tests classified as "high complexity" by the FDA, instead of using code G0434, which is the code for moderate complexity tests, which triggers a payment of approximately $20. Thus, the government alleges that federal healthcare programs paid CHS, and certain facilities under contract with CHS, approximately $80 more per test for the claims submitted with the higher-paying code.

The allegations arose from a lawsuit filed by a whistleblower who was a former laboratory director for CHS, under the qui tam provisions of the False Claims Act. He will receive $1.3 million from the settlement. ■

Survey: Most Health Providers Use No Cybersecurity Software

Most healthcare providers do not use any software for information security governance or risk management to protect against cyberattacks, according to a recent survey, which also found providers fear their own employees the most.

Ninety-five percent of healthcare organizations use no software for those functions, and 68% do not have a separate cybersecurity function, according to the Netwrix 2017 IT Risks Report, published by Netwrix Corporation, a data security company in Irvine, CA.

The results are based on feedback provided by IT specialists working for healthcare organizations around the globe. *(The report is available online at: http://bit.ly/2wJzQHl.)*

The survey also found that 56% of responding healthcare organizations perceive employees to be the biggest threat to system availability and security, 59% have had to deal with malware, and 47% have had security incidents caused by human error. Only 31% of healthcare organizations claim to be well prepared to beat IT risks.

Most healthcare organizations indicated lack of budget (75%), time (75%), and appropriate participation of senior management (44%) as the main obstacles to more efficient cybersecurity.

Healthcare providers may be starting to take the threat of cyberattacks more seriously, says **Michael Fimin**, CEO and co-founder of Netwrix. He notes that 56% of responding healthcare organizations say they plan to invest in security solutions to protect against data breach.

"While healthcare organizations continue to struggle with compliance and system availability, the security of electronic health records remains their biggest concern by far. Despite the surge in malware attacks and the high price that healthcare records command on the black market, the healthcare industry still sees employees as the main threat to the security of their assets," he said in a statement. "Even though most employees do not have malicious intent, organizations need to gain visibility into user activity across the IT infrastructure. Having a clear understanding of what is going on in the environment will help them mitigate the risk of human errors, detect and investigate incidents faster, and, as a result, improve the security of their sensitive patient data." ■

COMING IN FUTURE MONTHS

- Establishing audit trails
- Making your case for advancement
- Unexpected data security weaknesses
- Form responses to subpoenas

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 on to AHCMedia.com to take a post-test. Click on "My Account" to view your available CE activities. First-time users must register on the site using the subscriber number printed on their mailing label, invoice, or renewal notice.

3. Pass the online tests with a score of 100%; you will be allowed to answer the questions as many times as needed.

4. After successfully completing the test, a credit letter will be emailed to you instantly.

5. Twice yearly after the test, your browser will be automatically directed to the activity evaluation form, which must be completed to receive your credit letter.

CME/CE QUESTIONS

1. **Of the 412 people across 41 federal districts in the largest-ever healthcare fraud enforcement action by the Medicare Fraud Strike Force, how many were doctors, nurses, and other licensed medical professionals?**

   a. 115
   b. 215
   c. 312
   d. 412

2. **What issue is likely associated with many of the health professionals charged by the Medicare Strike Force, according to Jesse Witten, JD, partner with the law firm of Drinker Biddle in Washington, DC?**

   a. Drug diversion
   b. Malpractice
   c. Fraudulent licensing
   d. Improper training

3. **What is one challenge to identifying top-performing workers' compensation physicians, according to Linda Lane, president of Harbor Health Systems?**

   a. Obtaining physician buy-in
   b. Properly identifying physicians who may be listed under several name variations
   c. Eliminating physician data that does not involve workers' comp
   d. Obtaining current data

4. **What is one way consumerism creates additional risk for healthcare providers, according to Jane Harper, CISSP, CRISC, CRCMP, ISA, PCIP, CISA, ITIL, director of privacy and security risk manager at Henry Ford Health System?**

   a. Higher deductibles may lead more healthcare providers to set up credit plans, creating credit risk.
   b. Patients with financial trouble are more likely to sue for malpractice.
   c. Patients are more likely to scrutinize data security.
   d. Government agencies are responding more to consumer complaints about healthcare providers.

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

Misdiagnosis Leads to Sepsis, Amputations, and $16.5 Million Verdict

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

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

***Morgan Lynch**, 2018 JD Candidate*
Pepperdine University School of Law
Malibu, CA

News: In Wisconsin in mid-2011, a woman suffered gangrene, resulting in the amputation of her four extremities. The cause of the gangrene was a septic infection resulting from an untreated infection that was not disclosed to the patient, or treated. At trial, the jury awarded the patient $15 million, and her husband $1.5 million for loss of consortium.

Before and after the trial, the parties presented arguments about the validity of a Wisconsin statutory cap on noneconomic damages. The cap was found to be unconstitutional on its face because it was "not rationally related to curtailing the practice of defensive medicine," although this decision may be subject to further litigation.

Background: In May 2011, a woman presented to a Milwaukee ED for abdominal pain and high fever. The patient was seen by a physician and a physician assistant. The physician assistant included infection in his differential diagnosis, but admitted at trial that the patient met the criteria for systemic inflammatory response syndrome. Neither medical professional informed the patient about the diagnosis or the availability of antibiotics as treatment. The patient instead was instructed to follow up with her personal gynecologist for her history of uterine fibroids. The patient's condition deteriorated.

THE CAP WAS FOUND TO BE UNCONSTITUTIONAL ON ITS FACE BECAUSE IT WAS "NOT RATIONALLY RELATED TO CURTAILING THE PRACTICE OF DEFENSIVE MEDICINE."

The next day, the patient visited a different ED, where she was diagnosed with a septic infection caused by the untreated infection. The patient entered a coma and eventually became minimally responsive, and was transferred to another medical facility. Ultimately, the sepsis caused failure of almost all the patient's organs and led to dry gangrene in all four extremities, necessitating the amputation of all of her extremities.

The patient and her husband sued the physician, physician assistant, an insurance company, and the Wisconsin Injured Patients and Families Compensation Fund, alleging medical malpractice and failure to provide proper informed consent.

Fund representatives filed a pretrial motion to consider constitutionality. The circuit court addressed whether the statutory cap on noneconomic damages, as stated by § 893.55(4)(d)1, was unconstitutional. The circuit court held that the cap was not facially unconstitutional, but allowed the plaintiffs to raise an as-applied challenge to the cap post-trial.

After a lengthy trial, the jury found that both medical professionals failed to provide the patient with the proper informed consent regarding her diagnosis and treatment options. The jury awarded the patient $15 million in noneconomic damages, and awarded her husband $1.5 million for loss of consortium.

Post-verdict, the fund moved to reduce the jury award to the $750,000 statutory cap on noneconomic damages. The

plaintiffs moved for entry of judgment on the verdict, arguing that an application of the cap would violate their constitutional rights. They also renewed their pretrial facial challenge to the cap. The parties again fully briefed the constitutional issues and the circuit court reconsidered the constitutional questions.

The circuit court determined that the cap was not facially unconstitutional, but was unconstitutional as applied in this case because it violated the patient's rights to equal protection and due process. Both parties appealed the constitutionality rulings.

On appeal, the Wisconsin Court of Appeals relied heavily on *Ferdon ex rel. Petrucelli v. Wisconsin Patients Comp. Fund*, *2005 WI 125*, a 2005 Wisconsin Supreme Court case that stands for the proposition that statutory caps are unconstitutional when their justifications are "so broad and speculative that they justify any enactment." The Wisconsin Supreme Court instructed that courts, in determining the constitutionality of a statutory cap, should note that "while the connection between means and ends need not be precise, it, at least, must have some objective basis."

In reaching its decision, the Wisconsin Court of Appeals noted that the cap had "the practical effect of imposing devastating costs only on the few who sustain the greatest damages and create[d] a class of catastrophically injured victims who are denied the adequate compensation awarded by a jury, while the less severely injured malpractice victims are awarded their full compensation." Thus, the court ruled that the statutory cap was unconstitutional on its face and violated the couple's due process rights. The appellate court ultimately affirmed the circuit court's judgment, reinstating the original noneconomic portion of the jury award.

What this means to you: The facts of this case show clearly the importance of adhering to informed consent standards. It is vital that hospitals create informed consent policies that carefully track the case law and medical standards in the relevant jurisdictions and medical communities. Providing continuing medical education on changes to informed consent policies is another means of ensuring compliance and avoiding liability.

To elaborate on the background relevant here, the prevalence of undiagnosed severe sepsis and septic shock among patients in EDs led to the development of screening tools for sepsis, such as the "sepsis bundle" and a standardized diagnostic algorithm that regulatory and accreditation organizations require to be used during the assessment of all patients presenting to EDs. A high fever with abdominal pain signals a "hot abdomen" and requires an immediate surgical consult, as the probability of a bowel content leakage into the sterile abdominal cavity is high. The ensuing infection spreads rapidly into the bloodstream.

Primary sepsis (a direct infection of the blood, usually through injection using contaminated needles) or secondary bacteria in the bloodstream, usually from an untreated or incorrectly treated infection of soft tissue or bone, will become severe quickly and lead to septic shock, a life-threatening situation with a poor prognosis, especially in the very young, elderly, and patients with multiple comorbidities. The lack of communication of findings to the patient, compounded with the lack of screening for sepsis or even the most basic treatment — such as obtaining cultures and beginning broad-spectrum antibiotics — is a serious breach of multiple standards of care and led to the devastating consequences this patient and her spouse will continue to endure for as long as she survives.

Given the recency of this case, it is unclear if it will be appealed to the Wisconsin Supreme Court, although the importance to the medical community would suggest appeal is likely. It would be wise for medical professionals to support such an appeal to avoid an influx of future medical malpractice cases. Attorneys in Wisconsin reported refusal of medical malpractice cases based on the statutory cap at issue in this case. Notably, four of seven of the current Wisconsin Supreme Court justices began their terms post-*Ferdon*, and thus the judicial climate may have changed since the 2005 case. The state legislature's stated purpose in enacting the statute was "to ensure affordable and quality healthcare for Wisconsin residents, while also ensuring that victims of medical malpractice are adequately compensated."

As the court noted in this case, the very same purpose was rejected by the Wisconsin Supreme Court in *Ferdon*. Further, the alleged connection between the stated purpose and the statutory cap paralleled that of the contested *Ferdon* statute: the existence or nonexistence of "caps on noneconomic damages [does] not affect doctors' migration;" "defensive medicine cannot be measured accurately and does not contribute significantly to the cost of healthcare;" "the correlation between caps on noneconomic damages and the reduction of medical malpractice premiums or overall healthcare costs is at best indirect, weak, and remote;" and the cap was not necessary to the financial integrity of the fund. For a Wisconsin medical malpractice statutory cap to be sustainable given the Wisconsin Supreme Court's *Ferdon* decision, a different connection between the purpose of the statute and

the statutory cap or evidence showing the value of statutory caps likely will be required for a successful further appeal.

More broadly, this case illustrates that the national debate over statutory caps for medical malpractice continues. In the wake of a 2015 Nevada Supreme Court case upholding the Keep Our Doctors in Nevada Initiative, a $350,000 statutory cap that gained overwhelming voter support, several articles have praised the initiative's success in solving the Nevada medical crisis by keeping insurance rates low and retaining physicians. Similarly supportive of medical malpractice caps is the fact that more than half of U.S. states have enacted such caps, suggesting that state legislatures across the nation see the benefit of limiting noneconomic damages. It is important to bear in mind that damages caps vary by state, and it is advisable to consult with counsel who are well-informed about the laws in the relevant state concerning any particular situation. ■

REFERENCE

Decided on July 5, 2017, in the Court of Appeals of Wisconsin, Appeal No. 2014AP2812.

Medical Malpractice Case Disguised as Fraud Dismissed

News: In 2011, a woman presented to a Missouri medical clinic for treatment relating to her inflamed gallbladder. During a diagnostic scan, the patient was injected with substances that ultimately caused her tremendous discomfort and psychological trauma. She filed suit against the medical clinic, claiming that alleged representations made by unidentified medical professionals amounted to fraud. The trial court granted the defendant's motion to dismiss, finding the patient to have filed the petition untimely.

The patient appealed to the Missouri Court of Appeals. The court noted that the allegations in the complaint were essentially a medical malpractice claim disguised as a fraud claim. Accordingly, the court affirmed the dismissal of the petition with prejudice.

Background: On March 8, 2011, a woman was admitted to the nuclear medicine clinic in Missouri for a hepatobiliary scan to investigate inflammation in her gallbladder. Unidentified nurses and technicians injected the patient with an unknown substance or substances to trace and identify the abnormalities that were causing abdominal pain. When the substance was injected, the patient suffered an extreme burning sensation beginning in her left arm, spreading throughout her entire body.

Through its unidentified nurses and technicians, the clinic made representations that medical records of the procedure were being prepared and maintained at the time of the procedure as part of the hepatobiliary scan. According to the petition, the employees made these representations by "asking questions and recording [on the clinic's computer system the patient's] responses to those questions and the activities taking place in the treatment room."

Through its chief medical officer, the clinic represented that no medical records of the procedure were prepared or maintained at the time of the procedure on March 8, 2011. The patient claimed that the representations by the employees that medical records were being prepared and maintained were false.

The patient sued for fraud, alleging that the representations regarding the medical record were material to her decision to continue with the hepatobiliary scan; that the clinic knew or should have known that the representations were false; that the clinic intended that she would act upon the representations, and she acted in the manner reasonably contemplated by the clinic when she consented to continue with the hepatobiliary scan; that she was ignorant of the falsity of the representations; that she relied on the representations being true when she decided to continue with the scan; that she had the right to rely on the representations; and that, due to the lack or absence of medical records, she could not reasonably discover whether she had a cause of action for medical malpractice.

The patient further alleged that the clinic's conduct proximately caused her physical and psychological conditions, including seizures and PTSD, caused by the unknown substance(s). In response, the clinic filed a motion to dismiss the petition, alleging that the patient was attempting to circumvent the applicable statute of limitations for medical malpractice claims by characterizing her claim as a fraudulent misrepresentation claim, rather than a medical malpractice claim.

The circuit court granted the motion, agreeing that the patient

was attempting to reframe a medical malpractice claim into a fraud claim and holding the plaintiff's claim time-barred. The circuit court also found that, even if the claim was truly for fraud, the petition failed to set forth facts supporting each element for a fraud claim. Thus, the circuit court dismissed the petition with prejudice, and the plaintiff appealed.

The Missouri Court of Appeals inquired into whether the "gist or gravamen" of the patient's complaint was a claim for medical malpractice or fraud. In its analysis, the court put emphasis on the causation element pleaded by the patient, stating "[t]he source of the damages that [the patient] contends were proximately caused by [the clinic's] actions were not caused by any alleged misrepresentations, but by the unknown substance being injected into her arm." Thus, the court determined that the gist or gravamen of the petition was a medical malpractice claim. With that finding in mind, the court computed the applicable statute of limitations to have expired on March 8, 2013. Because the plaintiff failed to bring her claim until March 5, 2016, the court affirmed the trial court's dismissal with prejudice.

What this means to you: This case illustrates the importance of careful pleading. Had the plaintiff's attorney pleaded the case as a medical malpractice claim, the case would have been dismissed without an argument. The attorney's creative pleading gave the plaintiff a chance at recovery, which she had forfeited years ago. The obvious lesson for the defense is to carefully evaluate complaints and petitions to ensure medical malpractice claims cannot unlawfully sneak into court outside the applicable statute of limitations via a disguised fraud claim or otherwise. Of particular relevance was the court's focus on the causational element of the petition. It appears the gist or gravamen of a petition or complaint is contained in its causation allegations. Keeping this in mind, practitioners should focus their evaluations and arguments on causation to effectively refute plaintiffs with questionable claims.

The discovery rule (not triggering the statute of limitations until the plaintiff knows or should know about the claim) in the pleading context was subtly involved in this case. The plaintiff claimed that she was ignorant of the falsity of the representations made by the medical professionals. Such an argument may have provided the plaintiff tolling of the medical malpractice statute of limitations had she argued that she was unaware of the damage caused by the injections. Of course, it would be a difficult argument to make, given the instant burning sensation she experienced, but other cases may turn on the discovery rule. Taking this into consideration, defendants must evaluate whether potential plaintiffs have had the opportunity to learn the ultimate facts that establish the elements of their claims. If not, the standard expiration of a statute of limitations may not end a plaintiff's right to sue, and could create future litigation.

This case also demonstrates the value in maintaining proper medical records. Those records would have shown what substances were injected and by whom. Titles and credentials also would be indicated. However, the patient's complaint of burning at the initiation of treatment should have resulted in the immediate cessation of treatment, notification to the radiologist, and providing antidote treatment to the patient to prevent long-term consequences. Before injections of radioactive isotopes, dyes, and other diagnostic and contrast materials, a thorough review of the patient's allergy history and a discussion about any issues with similar previous procedures must occur and be well-documented, along with the patient's consent to have the substances injected. It is the responsibility of the radiologist to inform the patient about the procedure and the possible risks involved. There should be no unknowns, and if there are, the procedure should be delayed until all the patient's questions are answered. This informed consent process must be spelled out and documented clearly in the medical records to protect all those involved.

It is unlikely any exchange of documents occurred in this case, considering its early adjudication and defense victory on legal grounds. It is unclear whether the clinic kept the record the plaintiff alleged should have existed. The patient was entitled to her official medical record, but additional documentation could have been uncovered in discovery during litigation. The medical professionals would hope to seek protection in the records, showing any injections were within the standard of care. If the injections were improper, the clinic ran a tremendous risk of inviting a lack of informed consent claim for failing to disclose the contents of the injections and their effects, and were bailed out in this instance by the plaintiff's failure to act on a timely basis. Regardless, knowledge of the contents of any injection is important for defending a medical malpractice claim, and the importance of maintaining a detailed medical record cannot be overstated. ■

REFERENCE

Decided on May 23, 2017, in the Missouri Court of Appeals, Western District, Case No. WD 80063.

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Myriad State Requirements Complicate Breach Response

When you realize there has been a breach of protected health information (PHI), your first thought is of HIPAA and how to satisfy federal requirements for responding. But that is far from the end of your obligation, as state requirements can be just as onerous.

And if you do business in more than one state, the response can be especially burdensome because state laws requiring data breaches can be radically distinct — each requiring something different and, in many cases, specifically tailored to that state's government, notes **Nathan A. Kottkamp**, JD, a partner with the law firm of McGuireWoods in Richmond, VA.

Alabama and South Dakota are the only states that don't have data breach notification laws.

"There is a crazy quilt of 48 different state laws that come into play. Many of them layer on HIPAA, so that comes into play, but just complying with the breach requirements of HIPAA is not enough to comply with all these state laws," Kottkamp says. "What ends up happening is that if you have pure PHI for HIPAA purposes, just health information and name, in almost all of those cases all of these state laws are not going to come into play because they are focused on financial information. However, in many situations where there is a breach of PHI, the contents of that PHI are broader than just pure health information. They might involve account information, or a deductible, or a credit card that was used to pay for that healthcare."

> "THERE IS A CRAZY QUILT OF 48 DIFFERENT STATE LAWS THAT COME INTO PLAY... JUST COMPLYING WITH THE BREACH REQUIREMENTS OF HIPAA IS NOT ENOUGH TO COMPLY WITH ALL THESE STATE LAWS."

The inclusion of any information like that most likely triggers state law requiring breach notification, he says. Then things get complicated. For instance, there are wide variations in state law and nuances about exactly how a breach notification letter must be worded.

"There are state requirements that you must send a letter to their respective attorney general or consumer affairs division prior to sending it out to those affected by the breach. There is a small number that require the state actually bless the letter before sending it to those people," he says. "Then there are the timing issues, and with HIPAA, 60 days is your outside limit. But 45 days in at least two states, and Florida has the current record for the tightest, which is 30 days. You can really get yourself tripped up if you are laser focused on HIPAA and send your notification letter, but if, for instance, you forget to send the required statement about putting a credit freeze on your account as is required in six states and given a nod in other states."

In addition to listing all sorts of universal contact information like the Federal Trade Commission and credit reporting agencies, Maryland and North Carolina require that the breach notification letter include state-specific information for contacting the attorneys general in those states.

"If you have a 50-state breach, you can't use the exact same breach letter for everyone affected by the breach unless you want to tell people in Idaho how to contact the

attorney general in North Carolina, which doesn't make much sense," he says. "People like to think they can use a broad notification letter that covers everything that any state could possibly require, but then lo and behold, they've missed something like that state-specific requirement."

Many states also have supplemental requirements within their state agencies, Kottkamp notes. Whereas most states require that you notify the attorney general, some also specifically require that you additionally and separately notify another agency such as the department of consumer affairs.

States also have different thresholds for when you must notify the attorney general and other departments in those cases. Some states require reporting only if the breach affects more than 500 people, Kottkamp notes, while others set the trigger at 750 or 1,000.

"If you have a multistate affair with more than just health information, you literally have to go state by state to make sure you're checking all the boxes," Kottkamp says. "Some smaller healthcare providers won't have to deal with a breach in multiple states, but larger health systems and other kinds of operations in the healthcare industry are going to find that a breach of any size is likely to involve people in more than just the one state where the company resides or is headquartered."

Even large organizations can overlook the risk related to state breach notification requirements, Kottkamp warns. A hospital or health system may have a solid plan for fulfilling HIPAA breach notification requirements but only address state requirements as an afterthought, assuming the federal compliance automatically satisfies the state or that state requirements are comparatively minor.

New York Goes After Delayed Notice

That is not at all reliable, and the consequences can be serious. States take their breach notification laws seriously, as evidenced by the New York attorney general's recent settlement with CoPilot Provider Support Services, Kottkamp says. CoPilot, which provides support services to the healthcare industry, waited more than a year to provide notice of a data breach that exposed 221,178 patient records.

The company blamed the delay on an ongoing investigation by the FBI, but agreed to pay $130,000 in penalties and to improve its notification and legal compliance program, the Department of Justice announced.

On Oct. 26, 2015, an unauthorized individual gained access to CoPilot's confidential patient reimbursement data via the website administration interface and downloaded reimbursement-related records for 221,178 patients. In mid-February 2016, the FBI opened an investigation at CoPilot's request, focusing on a former CoPilot employee. On Jan. 18, 2017, CoPilot began to provide formal notice to affected consumers in New York, more than one year after CoPilot learned of the breach of patient data.

"You're looking at audits and other sorts of regulatory actions by the states if you don't comply. If the state requires you to notify its attorney general and you don't, the state will see the breach when it comes up on the federal government's list of large breaches," Kottkamp says. "Then, they're going to contact you and ask why you didn't notify them. That's a big problem. That's an open invitation for the state attorney general to just come in and hammer that provider."

The most aggressive states are likely to be the ones with the toughest cyber laws, so the top of the list would include New York, Florida, California, Illinois, Ohio, and Massachusetts, Kottkamp says. Massachusetts also has an oddball statute that, unlike how almost every other state requires the provider to describe what happened in the breach, specifically prohibits the provider from describing the breach.

"I don't know if they're worried about copycats or what, but it's a bizarre law," he says. "That's a great example of how you might think you're doing the right thing because it's the obvious thing and what every other state requires, but you do that in Massachusetts and you're in trouble."

Any state with an outlier requirement — like Maryland and North Carolina with their requirement for notifying specific agencies, and Ohio with its 45-day time limit — are likely to be more aggressive about enforcement, Kottkamp says. They know those are unusual requirements and they will check to make sure you paid attention.

Risk managers and compliance officers should maintain a list of applicable breach notification laws for every state in which the organization does business, Kottkamp suggests. That may be a long list for many covered entities, even relatively small ones, he says.

"Whenever there is a breach and it's more than just pure PHI, one of the top five questions to ask is what states are affected," he says. "Then,

you pull the breach notification laws for those states and start layering. The sort of stained glass window you end up with dictates what you need to do for breach notification, and you may find that you have to write several letters and send to many different places by different deadlines."

One source for the state breach notification laws is a compilation by the National Conference of State Legislatures, which can be found online at: http://bit.ly/1ao7NAi. Several law firms also have compiled state-by-state guides, such as one by the firm Foley & Lardner, which is available online at: http://bit.ly/2vkPfzd. ■

SOURCE

- **Nathan A. Kottkamp**, JD, Partner, McGuireWoods, Richmond, VA. Telephone: (804) 775-1092. Email: nkottkamp@mcguirewoods.com.

New Breach Reporting Tool Helps With HIPAA Response

A new breach reporting tool should be useful for HIPAA compliance, partly because it can help providers stay on top of what is currently trending in cyberattacks and other types of breaches.

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently launched the revised web tool, saying it puts important information into the hands of individuals, empowering them to better identify recent breaches of health information and to learn how the breaches are investigated and successfully resolved. The HIPAA Breach Reporting Tool (HBRT) features improved navigation for both those looking for information on breaches and ease of use for organizations reporting incidents.

The tool also educates on the types of breaches that are occurring, industrywide or within particular sectors, and how breaches are commonly resolved following investigations launched by OCR. The tool is available online at: http://bit.ly/1FrWfKp.

HHS Secretary **Tom Price**, MD, said HHS heard from the public that it needed to focus more on the most recent breaches and clarify when entities have taken action to resolve the issues that might have led to the breaches. "To that end, we have taken steps to make this website, which features only larger breaches, a more positive, relevant source of information for concerned consumers," he said.

HHS OCR originally released the HBRT in 2009, as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. It features public information that HIPAA covered entities report to OCR when they are involved in breaches of unsecured protected health information of 500 or more individuals. The tool includes the name of the entity, the state in which the entity is located, the number of individuals affected by the breach, the date of the breach, type of breach (such as a hacking/IT incident, theft, loss, unauthorized access/disclosure), and location of the breached information (such as a laptop, paper records, or desktop computer).

New features of the HBRT include enhanced functionality that highlights breaches currently under investigation and reported within the last 24 months; a new archive that includes all older breaches and information about how breaches were resolved; and improved navigation to additional breach information.

HHS said it plans to expand and improve the site over time to add functionality and features based on feedback.

HIPAA compliance leaders should find the improved tool useful, says **Jennifer R. Breuer**, JD, partner with the law firm Drinker Biddle in Chicago.

"OCR has always posted the wall of shame, the list of people with breaches — so it is the same tool we've had before, but more useful. The tool makes it easier to find the same information that was there before if you really took the time to dig through it," Breuer says. "You're able now to use the search capabilities and better understand why breaches have happened."

The most useful part of the tool might be the ability to monitor trends in HIPAA breaches, Breuer says. An individual case may not be so instructive, but a pattern could be, she says.

"It's not so important to know that hospital A did something silly and now they're publicly scolded, but it is important that you get a sense of how breaches are happening, the way in which your counterparts are falling prey to this problem that you're all trying to avoid," she says.

Seeing that one provider had trouble when an employee took a laptop home might not mean that

much, but if you see that several providers had breaches in the same way over a similar period of time, you might decide it is wise to take a look at your laptop policy, she says.

"You can see how people are actually accessing data inappropriately, and though some will be ways we all know about, some of the ways are evolving over time. You can get a better sense of the phishing and other attempts from external sources who are trying to access protected data," Breuer says. "You want to know what the risks are today, because they are changing over time."

Breuer's study of the data in the tool suggests there are plenty of the known human error-type breach causes, but there appear to be more phishing attempts and other outside attacks.

"It's a good reminder that both are still a threat and that you need to educate your people on the whole range of things that can result in data breaches," Breuer says. "There can be a tendency to think that this is a well-known issue among healthcare professionals and they know about all the standard ways you can have a data breach, so you only need to talk about cyberattacks. Or it can go the other way, but the truth is revealed when the data show that both still should be subject of your education efforts." ■

SOURCE

- **Jennifer R. Breuer**, JD, Partner, Drinker Biddle, Chicago. Telephone: (312) 569-1256.

Per-record Cost of Data Breaches Increasing

The cost of healthcare data breaches continue to remain the highest out of any industry, with an average cost of $380 per record, according to a recent report from the Ponemon Institute. Across all industries, the average cost for each lost or stolen record containing sensitive and confidential information decreased from $158 in 2016 to $141.

That means that a healthcare data breach costs 2.5 times more than the global average across other industries. The global average cost of a data breach is down 10% over previous years to $3.62 million. In the United States, the average cost for each lost or stolen record containing sensitive and confidential information across all industries increased from $221 to $225. The average total cost experienced by organizations over the past year increased from $7.01 million to $7.35 million.

However, companies are experiencing larger breaches. Globally, the average size of the data breaches increased 1.8% to more than 24,000 records, the report says. For all other industries, the average cost per record is $141.

The United States has a higher breach cost compared to Europe, which has shown a decline of 26% in cost year-to-year, with the difference attributed to the centralized regulatory environment in Europe. In the United States, organizations must adhere to federal and individual state regulations.

The report says the rise in breach cost also can be explained by the occurrence of HIPAA compliance violations and companies rushing to notify customers. The cost of issuing a notification of a breach alone is an average of $690,000 in the United States, which the report notes is twice that of any other country. The cost goes even higher when business associates are involved, increasing the cost by an additional $17 per record.

In the United States, Ponemon identified these factors that influence data breach costs: compliance failures, the extensive use of mobile platforms, chief privacy officer (CPO) appointment, and the use of security analytics. The use of security analytics reduced the per capita cost of data breach by $7.70 and the appointment of a CPO reduced the cost by $4.30.

"However, the extensive use of mobile platforms at the time of the breach increased the cost by $6.50, and compliance failures increased the per capita cost by $19.30," the report says. "Having an incident response plan and team in place, extensive use of encryption, employee training, BCM [business community management] involvement, and extensive use of data loss prevention technologies all reduce the cost of data breach by more than $9 per compromised record."

Data breaches due to third-party error, compliance failure, extensive migration to the cloud, rush to notify, and lost or stolen devices increased data breach costs by more than $10 per compromised record, Ponemon reports.

"To illustrate, a fully functional incident response team decreased the per capita cost of data breach from $225 to $199," the report says. "In contrast, third-party involvement in the breach incident increased the per capita cost from $225 to $249."

The full report is available online at: https://ibm.co/2rLVOKR. ■