HEALTHCARE RISK MANAGEMENT™

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

INSIDE

Enclosed in this issue:

Legal Review & Commentary: $17.6 million verdict for prescribing opioids at dangerous levels; medical team mistreats woman whose BP dropped dramatically after surgery

SEPTEMBER 2016 Vol. 38, No. 9; p. 97-108

Hospital Faces OCR Complaint For Gag Order on Abortion

A hospital in Washington, DC, is facing an investigation by the Health and Human Services (HHS) Office for Civil Rights (OCR) after a physician alleged that the facility barred her from speaking about abortion. The case raises important questions about how much a healthcare employer can restrict employees' private activities.

Ironically, the hospital cited a fear of encouraging anti-abortion protesters as the reason for keeping a low profile for its abortion services, but it is now in the news as an abortion provider.

Diane J. Horvath-Cosper, MD, an obstetrician-gynecologist and family planning fellow (FPF) at MedStar Washington Hospital Center in Washington, DC, is an outspoken abortion rights supporter. She performs abortions, and in 2015 she wrote an op-ed in *The Washington Post* about harassment from anti-abortion protesters and how she constantly feared for her safety.

Soon after that op-ed was published, Horvath-Cosper claims, MedStar administrators asked that she no longer speak publicly about abortion. *(The op-ed is available to readers online at http://wapo.st/2aZgZjY.)*

"A KEY ISSUE IN HER COMPLAINT TO THE OFFICE OF CIVIL RIGHTS LIKELY WILL BE WHETHER THE CHURCH AMENDMENT PROHIBITS THE HOSPITAL FROM DISCRIMINATING AGAINST THE DOCTOR."
— JOHN E. PETITE, JD, GREENSFELDER

The hospital's request came in December 2015, soon after a gunman killed three people outside a Planned Parenthood clinic in Colorado Springs, CO.

According to Horvath-Cosper's complaint, MedStar's chief medical officer explained that, for security reasons, the hospital did not want to draw attention to its abortion services. He allegedly told her he did "not want

Financial Disclosure: Author Greg Freeman, Executive Editor Joy Daughtery Dickinson, and Nurse Planner Maureen Archambault report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study. Arnold Mackles, MD, MBA, LHRM, physician reviewer, 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.

AHC Media

HEALTHCARE RISK MANAGEMENT™

Healthcare Risk Management™, ISSN 1081-6534, including HRM Legal Review & Commentary™ is published monthly by AHC Media, LLC, One Atlanta Plaza, 950 East Paces Ferry Road NE, Suite 2850, Atlanta, GA 30326

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 550669, Atlanta, GA 30355

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: AHC Media LLC is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation. This activity has been approved for 1.5 nursing contact hours using a 60-minute contact hour. Provider approved by the California Board of Registered Nursing, Provider #CEP14749, for 1.5 Contact Hours.

AHC Media is accredited by the Accreditation Council for Continuing Medical Education to provide continuing medical education for physicians. AHC Media 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 24 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.

EXECUTIVE EDITOR: Joy Daughtery Dickinson, (404) 262-5410. joy.dickinson@AHCMedia.com.
DIRECTOR OF CONTINUING EDUCATION AND EDITORIAL: Lee Landenberger.

EDITORIAL QUESTIONS
Questions or comments?
Call Editor **Greg Freeman**, (770) 998-8455.

to put a K-Mart blue light special on the fact that we provide abortions at MedStar." She claims in the complaint that, when she resisted the instructions to keep quiet, the department eventually threatened to fire her and that it "isolated" her. *(The complaint is available online at http://bit.ly/2aZppca. See the story in this issue for excerpts.)*

Church Law Cited

Horvath-Cosper worked with the National Women's Law Center and attorney **Debra S. Katz**, JD, of Katz, Marshall & Banks in Washington, DC, to file the complaint saying that the hospital violated the Church Amendment, a law that protects healthcare professionals at facilities that receive federal funding from being forced to violate their beliefs on abortion, whether they support or oppose the procedure. The Church Amendment usually is invoked by healthcare workers who refuse to participate in abortion procedures, Katz notes, but it is equally applicable in the Horvath-Cosper case. *(See the story in this issue for more on the Church Act.)*

MedStar released a statement saying it "is committed to providing family planning services for our community, and we do so in a respectful, private and safe environment. We look forward to cooperating fully with the Office for Civil Rights."

Political incentive?

The hospital sought to gag Horvath-Cosper not to ensure safety but for political reasons, Katz says.

"The hospital tried to ban a physician from speaking about a lawful medical procedure that is performed at the hospital, and they did it for improper political reasons," Katz says. "That stifled her ability to express her views about abortion as a legal medical procedure and, in effect, made it impossible for her to discuss important beliefs as a physician. The hospital denied her the full benefits of her position as a fellow by stifling her speech."

The complaint alleges that MedStar threatened to fire Horvath-Cosper if she continued to speak about abortion, even though she was not doing so at work and did not mention publicly that she worked at MedStar. Katz says, however, that the employer would not have been able to restrict the doctor's talk of abortion in the workplace either.

Horvath-Cosper and her attorneys approached hospital administrators about a solution that would allow her to speak about abortion on panels and in other

EXECUTIVE SUMMARY

A physician who says her hospital forbade her from speaking publicly about abortion has filed a civil rights complaint. The case raises questions about how much a healthcare provider can restrict an employee's public behavior.

- The hospital provides abortion, but administrators did not want to publicize that fact.
- The hospital cited security concerns as the reason for restricting her speech.
- No complaints were made until the doctor published an op-ed in *The Washington Post*.

professional settings.

"The response was no," Katz says. "That invariably led to having to elevate it to an OCR complaint."

MedStar may have trouble justifying its actions, says **Nannina Angioni**, JD, a labor and employment attorney and partner at the Los Angeles law firm Kaedian.

"If an employer implements broad brush strokes in describing what employees are prohibited from talking about, it may as well prepare for a lawsuit. Any limit on an employee's speech must be specifically and narrowly tailored to prohibit only disclosure of company confidential data, trade secret information, or private client information," Angioni says. "If an employer really wants to limit employee speech activities, it does so at great legal risk and must proceed with caution."

Attempting to bar speech related to personal views or feelings is difficult enough, Angioni says, but barring speech about common medical practices that routinely occur in healthcare settings is especially problematic. Employers cannot limit an employee's speech when the employee is off the clock or outside of work, Angioni says, unless, for example, an employee is breaching confidentiality or divulging trade secrets.

Though the Church Amendment was invoked in this case, Angioni says employees have other free speech protections. "Employees also have a right to speak about issues that affect the workplace or could be seen as supporting collective bargaining or a grievance related to a workplace issue. And while this language seems limited to very specific situations, it is not as clear-cut as you may think," she says. "The National Labor Relations Board has found speech activity protected in furtherance of such rights when, at first blush, it doesn't seem to fall into this category. I could see this issue being one in that category."

OCR Decision Uncertain

The applicability of the Church Amendment is not certain, says **John E. Petite**, JD, an attorney with the law firm Greensfelder in St. Louis. He has frequently litigated First Amendment issues and successfully defended defamation and privacy claims for healthcare providers.

He notes that the doctor is not alleging that she is being discriminated against for performing abortions. Rather, she is complaining that she is being discriminated against for her media advocacy on the topic of abortion.

"As a result, a key issue in her complaint to the Office of Civil Rights likely will be whether the Church Amendment prohibits the hospital from discriminating against the doctor for such media advocacy, even though it apparently does not discriminate against her for performing abortions," Petite says. "Even if HHS were to determine that the Church Amendment protected the complaining doctor's public advocacy, another issue as to the applicability of the Church Amendment might be whether that advocacy was the result of her 'religious or moral convictions,' as opposed to political convictions."

Petite says he suspects that OCR would find that the doctor's media statements could be ascribed to "moral convictions," which would support a violation of the Church Amendment.

If OCR rules in favor of the doctor, it probably will require the hospital to take corrective action, Petite says. Those actions could include changing a policy or procedure, restoring lost benefits, and providing notice to clients and employees that the hospital has taken steps to comply with a federal statute or regulation, he says.

If the hospital refuses to take corrective action, the next step would be for OCR to recommend initiating enforcement proceedings against the hospital, Petite explains. In the worst-case scenario, the hospital could lose all federal financial assistance because of the violation, he says.

"Although the federal government, were it so inclined, very likely could sue the hospital in federal court to enforce the Church Amendment, the doctor, as a private individual, likely could not," Petite says. "So far, the handful of federal courts that have looked at the issue have held that a person allegedly deprived of her rights under the Church Amendment does not have a private right of action to sue in federal court for that purported violation."

Doctor Can Sue

The doctor could try to sue under a federal statute, 42 U.S.C. § (1983), part of the Civil Rights Act of 1871, that vests individuals with a private right of action for violations of federal statutory or constitutional rights, such as the First Amendment or perhaps the Church Amendment, Petite says. However, that right of action is only available against "state actors." Only in very limited and relatively rare circumstances have courts held that a private entity or individual qualifies as a "state actor."

A lawsuit by the doctor would be an uphill battle. MedStar is a private actor, and courts generally refuse to hold that a private hospital is a state actor for purposes of § 1983 based solely on its receipt of federal funds, Petite says.

If the doctor were to sue the hospital in federal court directly

under the Church Amendment, under § 1983, or both, the hospital likely would move to dismiss her federal court complaint on these grounds, Petite says.

"Regardless of the viability of her claims or potential claims, the doctor may view her complaint to OCR and the media attention her complaint has attracted as insulation in and of itself against further actions by the hospital allegedly designed to silence her," he says. "Even putting aside the regulatory proceeding and the merits of the doctor's claim, now that this dispute has attracted media attention, the hospital has some thorny public relations issues with which to wrestle. Those issues create business risk apart from legal risk and may drive the hospital's ultimate decision on how best to respond to the doctor's complaint." ■

SOURCES

- **Nannina Angioni**, JD, Partner, Kaedian, Los Angeles. Telephone: (310) 893-3372. Email: nangioni@kaedianllp.com.
- **Debra S. Katz**, JD, Katz, Marshall & Banks, Washington, DC. Telephone: (202) 299-1140. Email: katz@kmblegal.com.

Complaint Alleges Effort to Silence Doctor

In the Office for Civil Rights complaint filed by Diane J. Horvath-Cosper, MD, an obstetrician-gynecologist and fellow at MedStar Washington Hospital Center in Washington, DC, she outlines what she says was an insistence by hospital administrators to stop her from talking publicly about abortion.

These are excerpts from the complaint:

• "On December 4, 2015, Dr. Gregory Argyros (Chief Medical Officer), in an alleged attempt to increase security at the Hospital, instructed Dr. Horvath-Cosper to immediately cease her media advocacy on the 'topic' of abortion, stating, *inter alia*, that he did not 'want to put a K-Mart blue light special on the fact that we provide abortions at MedStar.'"

• "Since this time, MedStar has prohibited Dr. Horvath-Cosper from accepting any media engagements on the topic of abortion and related women's health issues, threatened repercussions if she continued with her public abortion advocacy, directed her not to take legal action, isolated her within her Department, Obstetrics-Gynecology ('OB-GYN'), and forced her to choose between remaining employed and sacrificing the public advocacy that is central to her moral convictions about abortion and the primary reason she became an FPF at MedStar."

• "Upon information and belief, MedStar does not similarly restrict the speech of physicians in other specialties who seek to engage in media advocacy about their specialty or discriminate against them when they speak out." ■

Church Amendment Protects Abortion Views

The Church Amendment that a physician is citing in her claims that a hospital restricted her speech on abortion normally is invoked by healthcare providers on the other side of the controversial issue, says **John E. Petite**, JD, an attorney with the law firm Greensfelder in St. Louis.

Congress enacted the Church Amendment after the U.S. Supreme Court's 1973 decision in *Roe v. Wade*, in response to concerns that federal law could be interpreted to require individuals and healthcare delivery systems to provide abortions or sterilizations against their will, he says. The Church Amendment was intended to protect the so-called "conscience rights" of healthcare workers and institutions with respect to those procedures.

"The federal statute prohibits any healthcare entity that receives certain federal funding from requiring a physician or other healthcare personnel to perform an abortion or sterilization procedure contrary to the individual's religious or moral convictions," he says. "It also prohibits discrimination in the terms of employment against such individuals who either participate or refuse to participate in those procedures."

The amendment protects "entities that object to performing or assisting in the performance of abortion or sterilization procedures if doing so would be contrary to the provider's religious beliefs or moral convictions." It also extends protections to personnel decisions and prohibits any entity that receives a grant, contract, loan, or loan guarantee under certain statutes from discriminating against any healthcare personnel in employment because the individual performed or refused to perform an abortion, if doing so would be contrary to the individual's religious beliefs or moral convictions. ■

Caution: Patients' Printed Records May Not Match the Electronic Health Record

Most plaintiffs' attorneys now request audit trails immediately with the first contact for e-discovery, and risk managers often groan when they think of the work involved. However, there is a reason to seek the audit trail for your own benefit: It might show more exculpatory evidence than a paper printout of the same file.

Even with an automated auditing system, it may be time-consuming and burdensome to request the audit trail from the IT department and verify the facts of the case. However, it is almost always worth the trouble, says **Catherine J. Flynn**, JD, an attorney with the law firm of Carroll McNulty Kull in Basking Ridge, NJ.

An audit trail provides a record of every time the document was accessed or transferred, and it can be the best defense to claims of incomplete or misleading e-discovery. While sometimes burdensome to put together, the audit trail can be invaluable, she says.

"We're finding that the audit trail is more friend than foe in litigation, especially if there is a charge that the file has been amended or altered," Flynn says. "The audit trail will establish, for example, that the charting was done contemporaneously, in real time. It gives us valuable information and helps us establish that the documentation is as it should be."

That position is particularly important when electronic records are inconsistent with paper records, which is quite common in hospital litigation, says **Michael A. Moroney**, JD, also an attorney with the law firm. The information on the paper record may not necessarily conflict with the electronic health record (EHR), but it is likely to be incomplete and less clear.

"What the clinician is entering and reading on the electronic record is often vastly different from what we see on paper," Moroney says. "Information on a computer screen often does not translate well to a printed form, so even when you take that electronic record and print it out, you're not likely to get an exact copy of what the nurse or doctor was working with."

Audit Trail Saves Doctor

Flynn recalls a case a few years ago in which the plaintiff's attorney requested the client's record directly from the medical records department of a hospital before any lawsuit had been filed. The patient's record consisted of only one visit to the ED, and the medical records department had only the hard copy printout of the electronic record because that was what the ED routinely sent for filing.

The medical records department provided a copy of the printout to the attorney, and later the hospital realized that the printout omitted a key piece of information: that the patient did not comply with treatment and was discharged against medical advice (AMA), after being advised that doing so could result in paralysis. The doctor properly documented the AMA and warning in the electronic record, but it did not print on the hard copy.

The patient was paralyzed from the waist down a week after the ED visit. He sued the physician and told his attorney that he had complied with treatment and wanted to be admitted to the hospital. When the doctor received a subpoena, he went into the electronic record to confirm that he had properly documented the AMA and warning about paralysis. He couldn't understand why the patient was suing and why the plaintiff's attorney took the case. The doctor printed the medical record as proof of his actions, made sure that the AMA and warning appeared on the printout, and gave that hard copy to his attorney.

File Shows No Alteration

During interrogatories, the doctor's attorney provided the new printout showing the AMA.

"It appeared that the doctor had altered the medical record, adding the perfect defense to being sued," Flynn says. "The doctor swore that he entered that information before the patient ever left the building, but the first printed record was a pretty good argument that he had added that later."

EXECUTIVE SUMMARY

Audit trails can be an important defense in medical malpractices cases. The printed version of a file often does not match the electronic record.

- The paper record may be incomplete and less clear.
- Audit trails also can help with HIPAA compliance.
- Hospitals should have specific policies and procedures for e-discovery.

Flynn obtained the audit trail for the patient's record, which clearly showed the date and time the information was entered, which was before the time a nurse entered the time of discharge AMA. The plaintiff still resisted, so Flynn's firm had to convince a representative of the EHR vendor to give a deposition about how the system works and why the audit trail was conclusive proof that the doctor had entered the information at that time.

"The case was dismissed, but only after a lot of time and expense because on the first look, the situation did look very questionable," Flynn says. "At first blush, it did look like there was an addition to the chart two days after the physician was served. The lesson learned is that audit trails are not the enemy, even though they are sometimes perceived as onerous to put together."

Helpful with HIPPA

Audit trails also can be helpful addressing the new challenges and pitfalls of e-discovery. Previous policies and procedures on discovery may not be sufficient for complying with e-discovery, and risk managers should develop the necessary guidelines immediately, Flynn says.

E-discovery can be challenging, in part, because there are competing interests, Flynn says. The Health Insurance Portability and Accountability Act (HIPAA) requires hospitals to safeguard protected health information (PHI), but complying with e-discovery can sometimes involve that PHI.

"It puts the provider in a difficult position, trying to figure out how to satisfy all these compliance dictates," Flynn says. "There has to be a process by which you compile e-discovery, evaluate it, and make sure every step of the way that you're abiding by both the court rules, while still maintaining the HIPAA protection. Providers really struggle to make the marriage between the two a happy one."

The tension arises because evidence rules essentially require turning over all electronic documents related to the case, Moroney says. That requirement applies to all cases, but healthcare cases bring the HIPAA conflict.

"You have to turn over all evidence to your adversaries, and if you don't, both the client and the attorney can be in trouble," Moroney says. "You could be facing an amendment to a plaintiff's complaint alleging failure to turn over necessary medical records. So you have that on the one hand and, on the complete opposite side, is HIPAA saying you can turn over protected information only in limited circumstances."

Audits Show Compliance

Protecting PHI has become even more important in recent years as it became known that medical records are among the most sought-after documents for identity thieves, Moroney notes. At the same time, the adoption of EHRs greatly increased the amount of electronic PHI that any healthcare provider must protect.

Healthcare providers already have HIPAA compliance programs, but many need to assess those policies and procedures to makes sure they include the risk management department and e-discovery procedures, Flynn says. HIPAA education and compliance should address e-discovery and how to comply with both requirements, she says. In particular, emphasize that the e-discovery is not just about the EHR, but all documents involving patient care.

"There are documents that pertain to a patient but are not considered a specific part of the medical record, but are still maintained electronically and stored separately," Flynn says. "You must have specific e-discovery policies and procedures in place so that everyone knows these are the steps we take once e-discovery is undertaken."

Releasing information can be tricky, but hospitals also must preserve information that might be requested later. Once a lawsuit is filed, or there is a reasonable belief that there is a claim, most jurisdictions require the healthcare provider to maintain all documents and electronic information related to the case so that the evidence is available as the litigation proceeds.

Educate staff members about the need to preserve such information because their focus is likely to be on HIPAA compliance rather than evidence rules, Flynn says.

If there ever is an allegation that the hospital violated HIPAA — either as part of e-discovery or otherwise — an audit trail can be the best defense, Moroney says.

"Compliance with HIPAA is all about reasonableness, whether you took reasonable steps and established reasonable safeguards to protect patients' PHI," Moroney says. "The audit trail is like a history of your compliance efforts. It can show what you did and when you did it, who accessed a certain file and when. If you were reasonable in your compliance efforts, the audit trail can help prove that."

SOURCES

- **Catherine J. Flynn**, JD, Carroll McNulty and Kull, Basking Ridge, NJ. Telephone: (908) 848-6300. Email: cflynn@cmk.com.
- **Michael A. Moroney**, JD, Carroll McNulty Kull, Basking Ridge, NJ. Telephone: (908) 848-6300. Email: mmoroney@cmk.com. ■

You Must Respond Carefully When You Are Served With a Subpoena

Responding to subpoenas is a routine task for risk managers and general counsel, but just because it is routine doesn't mean it should be taken lightly. There are right and wrong ways to respond, and your actions at this early stage of potential litigation can affect the outcome later.

Subpoenas can demand that you turn over specific documents, and they also can require a person to appear in court. In either case, most of the same precautions apply.

First, you never should take the subpoena at face value and immediately comply, says **Christine G. Savage**, JD, an attorney with the law firm of Choate Hall and Stewart in Boston. A subpoena must be taken seriously, and failure to comply can result in punitive actions from the court, but the first priority is to ensure the validity of the document.

Start with determining where the subpoena originated. If it comes from a federal or state court, confirm that is signed by a judge or magistrate, Savage advises. If so, the subpoena carries the weight of a court order, she says. The hospital should provide the requested information, even if it is protected health information (PHI) covered by the Health Insurance Portability and Accountability Act (HIPAA).

The same rule applies if the subpoena comes from a law enforcement authority, such as a U.S. attorney's office, and cites a law enforcement or health oversight need. The hospital can comply with that subpoena without obtaining the patient's permission

If the subpoena is issued by a plaintiff's attorney in a civil matter, which Savage says is quite common, the hospital's response may be different. At that point, there could be a conflict with HIPAA, Savage says.

In most cases, PHI cannot be provided in response to an attorney's subpoena unless the patient has provided permission or a reasonable amount of time has passed without the patient objecting to the request.

> ... THE FIRST PRIORITY IS TO ENSURE THE VALIDITY OF THE DOCUMENT.

"There are a lot of aggressive civil litigators who will hound risk managers or the people in health information management, saying you have to respond to this subpoena by this deadline. But they don't send anything along with the subpoena indicating they have complied with the additional requirements of HIPAA," Savage says. "We spend a lot of time educating those people."

The case caption also can dictate how you respond. If the hospital or health organization is named in the subpoena's case caption, the subpoena should be referred to your senior management or legal counsel immediately.

"That suggests that the institution itself is being sued, so you want to have counsel look at it before you provide anything," Savage says. "If the institution is not named but the patient is named in the case caption, and usually even if they're not, we would reach out to the person who sent it and ask if they have tried to get the patient's authorization. If they haven't, we tell them we're going to."

An authorization from the patient can simplify the process, which prevents the need to assess what types of records are involved and how federal and state privacy protections apply, Savage says. Some records still can be released with the patient's permission, but a blanket authorization eliminates the time involved in assessing each type of record.

Only What's Required

When complying with a subpoena, be sure to provide only what was requested. In most states, for example, a subpoena must specifically ask for specially protected records such as those pertaining to mental health and substance abuse. A subpoena asking for all of a patient's medical records would not be

EXECUTIVE SUMMARY

Subpoenas require a careful response from a healthcare institution. Even a valid subpoena will be limited in what it requires.

- A court subpoena carries more weight than one from an attorney.
- The patient's authorization may be needed for the release of some documents.
- Do not provide more than what the subpoena requests.

sufficient to obtain those documents, Savage explains. The subpoena would have to ask for those records in particular and justify why they should be released.

Federal law makes substance abuse records especially hard to obtain in a subpoena, Savage notes.

"You have to get the patient's permission unless it is a law enforcement matter, and, even then, I would advise risk managers to talk to someone in senior management at the institution before complying," she says. "This kind of request signals that something else is going on, possibly something bigger than just this one patient and that could involve the hospital in some way."

Also, be careful not to volunteer that certain documents exist. If the patient has a history of substance abuse, for example, that information can be redacted, and you do not have to bring it to the other party's attention.

"However, you don't want to say that substance abuse records are specially protected, so you're not going to provide the patient's records from his stay in rehab," Savage says. "You've just told them that he was in rehab, and that alone is a breach. I've seen situations where well-meaning records staff have done that, asking, 'Were you seeking their mental health records in addition to the medical records?'"

Risk managers can work with legal counsel to write a subpoena and search warrant policy that outlines these precautions for anyone in the institution who might be in a position to receive those demands, Savage suggests. With search warrants, which often come in tandem with subpoenas, many of the same precautions apply. *(For more on search warrants, see the story in this issue.)*

Challenge Subpoena

In some cases, the hospital may want to file a motion with the court to quash the subpoena, says **Nicholas D. Jurkowitz**, JD, partner with the law firm of Fenton Law Group in Los Angeles.

"There may be reasons internally that a hospital would not want these records produced and would want to fight," Jurkowitz says. "There may be internal policies and procedures that you don't want out there or sensitive information that could be damaging to the hospital if it were to be made public. That's when you need a tactical assessment to determine if it's in the hospital's best interest to fight it."

Legal advice is always a good idea with a subpoena, he says. Jurkowitz once had a client who produced records in response to a subpoena before seeking legal advice, but problems arose between the two parties about what constituted compliance. By the time Jurkowitz stepped in, the original subpoena had been followed by court orders that were much more demanding and restrictive.

"They had just done it on their own, thinking they were doing the right thing by handing over the documents," he says. "Then problems arose, and we were really handcuffed by the court order that might have been avoided, or we might have been able to tailor the court order in a way that was more favorable to my client. We lost a lot of strategic options because mistakes were made very early."

Watch the Calendar

Once the subpoena is validated, pay attention to the calendar. Note the date by which the records are required, which sometimes can be too soon for the hospital to comply. It is not unusual for a subpoena to request records be delivered within a week, Savage says, and that deadline doesn't allow enough time if the patient must be contacted for permission.

"In those cases, I recommend just picking up the phone and talking to the lawyer or the law enforcement agency and asking for an extension," Savage says. "And you also want to put the onus back on them to obtain the necessary authorization. I also would tell them that if they don't do those two things, I will file a motion with the court to quash the subpoena."

A hospital can develop a form letter for responding to subpoenas, Savage suggests. The letter can summarize the HIPAA rules as they apply to subpoenas, along with information about specially protected documents and any state rules that may apply.

Savage cautions that you cannot ignore a subpoena, even if it is onerous or insufficient in some way. The subpoena may request specially protected information that you know you can't release, for example, but you still must respond. Failing to respond can result in the lawyer or law enforcement agency going to court and reporting that you failed to respond to a subpoena.

"That never looks good, even if the subpoena was faulty in the first place," Savage says. "At that point, you may get a court order requiring you to produce more than the original request, or you may be called into court to explain yourself to the judge." ■

SOURCE

- Nicholas D. Jurkowitz, JD, Partner, Fenton Law Group, Los Angeles. Telephone: (310) 444-5244. Email: njurkowitz@fentonlawgroup.com.

Search Warrants Don't Mean All Access for Police

Search warrants can be more intimidating than subpoenas because law enforcement officials show up at the facility and demand access to certain areas and documents. That event can lead some risk managers or other hospital leaders just to glance at the search warrant and wave the police officers in.

That response would be a mistake, says **Christine G. Savage**, JD, an attorney with the law firm of Choate Hall and Stewart in Boston.

"You don't let anyone take anything or rifle through files until you have verified the validity of the search warrant and its limitations," Savage says. "You call a senior administrator and ask the people with the search warrant to sit in a lobby or conference room where you can keep an eye on them."

If the search warrant is confirmed as valid, Savage recommends letting the staff in the targeted department leave for the day. If they remain in the department, or even nearby, the officials executing the search warrant will attempt to talk to them and obtain more information.

"It's always amazing to me how many people will talk to law enforcement without considering whether they need a lawyer or giving the institution the opportunity to assert that it represents all its employees and will get them a lawyer," Savage says. "There should be a senior administrator who is the point person, physically there with law enforcement officials, and that should be the person they talk to." ■

Doctor Challenges Medical Errors 'Hysteria'

A report calling medical errors the third leading cause of death has serious flaws that make that conclusion invalid, according to a physician. He says the report contributes to an irrational hysteria over medical errors.

The analysis in *The BMJ* received significant attention in the general media and within the healthcare industry, but it actually does not show such an impact from medical errors, says **Gerard Gianoli**, MD, FACS, a neuro-otology and skull base surgeon, and a clinical associate professor at Tulane University School of Medicine in New Orleans. Gianoli recently published a critique of the *BMJ* report in *The American Journal of Medicine (AJM). (The* AJM *article can be accessed online by going to the website http://bit.ly/2anG1cH.)*

Gianoli says the *BMJ* report was "inflammatory," "sensationalist," and that it was an opinion piece rather than a scientific study.

The *BMJ* report was the result of analyzing data after 1999 to determine a mean rate of medical error-related deaths at 251,454 per year. That rate was factored into the total number of U.S. hospital admissions in 2013, and, using those figures, medical errors were the third most common cause of death in the United States.

Documentation of Errors

The study was led by Martin Makary, MD, MPH, FACS, professor of surgery and health policy & management at Johns Hopkins University School of Medicine in Baltimore, MD. (*The* BMJ *report can be accessed by readers online at http://bit.ly/1rtW6Sa.) Healthcare Risk Management (HRM)* requested comment on Gianoli's criticism but did not receive a response from Makary.

The report also said that medical errors are not well documented in death certificates, and the researchers suggested that a new field be added to the certificates asking if the death was related to an avoidable complication of medical care.

Gianoli says the "third leading cause of death" claim is invalid because the number of patient deaths analyzed over 10 years was only 35.

"The paper simply states the average of three previously published studies and one paper that was never vetted through the peer review process — all published more than eight years ago," Gianoli says in the *AJM* report. "All four of these papers include a combined analysis of a grand total of only 35 actual patients, from which the authors extrapolate to

EXECUTIVE SUMMARY

A physician is challenging the validity of a recent report calling medical errors the third leading cause of death in the country. He suggests that such reports are encouraging an overreaction to medical errors.

- The original report included only 35 deaths.
- The definition of "medical error-related" is disputed.
- Some deaths are not caused by the medical error, the doctor notes.

251,454 deaths due to medical errors in the U.S. every year. This is a highly dubious estimate."

Errors Don't Always Kill

Gianoli tells *HRM* that he also questions how medical errors were defined for the analysis. Some deaths attributed to medical error were not caused by the error itself, he says. Even if a significant medical error occurred in the process of caring for the patient, it may have had no effect on the outcome, he says, but it might still be classified as "medical error-related." In other cases, a known potential complication can be misclassified as an error.

"When a patient was sent home from an emergency room in Dallas with Ebola last year, this was an error probably caused by electronic medical record-related disruption. The patient later returned and died. But he probably would have died even if this systems error had not occurred," Gianoli says in the paper.

Gianoli takes issue with the one case presented in the *BMJ* article. It concerns a patient who died of complications from pericardiocentesis, a procedure in which the surgeon inserts a needle into the sac around the heart. The procedure is risky, and complications are not unexpected, Gianoli says. The complication can occur without any overt error by the surgeon, he says.

The conclusions of the report are overstated because death would be inevitable in many cases without medical intervention, he says, and the margin of error in critically ill patients is often razor thin.

Gianoli thinks the *BMJ* article could contribute to an excessive focus on medical errors, which makes it "the silicone breast implant hysteria" of our generation. In the 1980s and 1990s, extensive media coverage and fearmongering about silicone breast implants resulted in many being removed without medical justification, and plaintiffs' attorneys benefited. A maker of the implants, Dow Corning, went bankrupt, and a moratorium was placed on the use of silicone, which kept it from patients who needed breast cancer reconstruction. Years later, medical research established that the fears were unfounded and silicone implants are safe.

Gianoli says he doubts the *BMJ* report will result in fewer medical errors, but he says that it could have a negative effect on healthcare if it leads to more administrative requirements and data collection. Healthcare professionals are willing to admit their errors and improve, Gianoli says, but he characterizes the *BMJ* report as "self-serving, irresponsible sensationalism by Monday-morning quarterbacks." ■

Largest HIPAA Settlement Ever for Advocate

The largest ever settlement of alleged violations of the Health Insurance Portability and Accountability Act (HIPAA) was made with the Chicago-based Advocate Health Care Network, one of the largest health systems in the country, which has agreed to pay $5.55 million and adopt a corrective action plan.

The Department of Health and Human Services, Office for Civil Rights (OCR) had sued Advocate for multiple potential violations involving electronic protected health information (ePHI). The settlement is the largest to-date against a single entity, and OCR says the size of the settlement was the result of the extent and duration of the alleged noncompliance. Some of the alleged violations dated back to the inception of the Security Rule.

The settlement amount also was influenced by the involvement of the state attorney general in a corresponding investigation, and the large number of individuals whose information was affected by Advocate, OCR Director **Jocelyn Samuels** said in announcing the resolution. "We hope this settlement sends a strong message to covered entities that they must engage in a comprehensive risk analysis and risk management to ensure that individuals' ePHI is secure," Samuels said. "This includes implementing physical, technical, and administrative security measures sufficient to reduce the risks to ePHI in all physical locations and on all portable devices to a reasonable and appropriate level."

OCR began its investigation in 2013, when Advocate submitted three breach notification reports pertaining to separate and distinct

COMING IN FUTURE MONTHS

- Unique settlement with plaintiff
- Effective walk-around strategy
- Trends in workers' compensation
- What earns the best premiums

incidents involving its subsidiary, Advocate Medical Group. The combined breaches affected the ePHI of about 4 million individuals. The ePHI included demographic information, clinical information, health insurance information, patient names, addresses, credit card numbers and their expiration dates, and dates of birth, OCR reports.

OCR's investigations into these incidents revealed that Advocate failed to do the following:

- conduct an accurate and thorough assessment of the potential risks and vulnerabilities to all of its ePHI;
- implement policies and procedures and facility access controls to limit physical access to the electronic information systems housed within a large data support center;
- obtain satisfactory assurances in the form of a written business associate contract that its business associate would appropriately safeguard all ePHI in its possession;
- reasonably safeguard an unencrypted laptop when left in an unlocked vehicle overnight.

Advocate Health Care Network is the largest fully integrated healthcare system in Illinois, with 10 acute-care hospitals and two integrated children's hospitals. ■

Largest Data Breach of 2016 Hits Banner Health

The largest data breach so far in 2016 happened recently when hackers obtained information on 3.7 million patients and others from the computer servers of Banner Health, based in Phoenix. The breach included not just financial data, but also sensitive information such as Drug Enforcement Agency (DEA) numbers, tax identification numbers, and national provider identifier numbers.

The breach included the servers that process payment card information where food and beverages are sold in Banner facilities. The compromised information includes patient names, addresses, birthdates, physician names, dates of service, clinical information, health insurance information, and Social Security numbers, according to Banner's announcement of the breach. Claims information from Banner's health insurance programs and employee benefit records also may have been taken, along with provider names and addresses.

Banner Health released a list of 27 food and beverage locations where the hackers had access to payment card data from June 23 to July 7. When the breach was discovered, Banner temporarily stopped accepting credit and debit cards at those locations until the system was deemed secure again. In addition to offering free credit and identity monitoring to those affected, Banner notified the DEA and providers' licensing boards of the incident because the compromised DEA numbers and national provider numbers could be used fraudulently and connected to the license holders. ■

'Widespread Vulnerabilities' Bring $2.7M Settlement

Oregon Health & Science University (OHSU) in Portland has agreed to settle potential Health Insurance Portability and Accountability Act violations with a $2.7 million fine after an investigation by the Office for Civil Rights (OCR) found "widespread and diverse problems" at OHSU.

OHSU must adhere to a three-year corrective action plan.

The investigation was prompted when OHSU submitted multiple breach reports affecting thousands, including two reports involving unencrypted laptops and another large breach involving a stolen unencrypted thumb drive.

OCR's investigation uncovered evidence of "widespread vulnerabilities" within OHSU's compliance program, including storage of the electronic protected health information (ePHI) of more than 3,000 individuals on a cloud-based server without a business associate agreement. The resolution agreement and corrective action plan are available to readers online at http://bit.ly/29PjtTf. ■

CE/CME OBJECTIVES

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

1. describe the legal, clinical, financial, and managerial issues pertinent to risk management;
2. explain the impact of risk management issues on patients, physicians, nurses, legal counsel, and management;
3. identify solutions to risk management problems in healthcare for hospital personnel to use in overcoming the challenges they encounter in daily practice.

HEALTHCARE RISK MANAGEMENT™

CE/CME 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. Scan the QR code to the right or log on to the AHCMedia.com site to take a post-test. Go to "My Account" to view your available CE activities. First-time users will have to 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.

CE/CME QUESTIONS

1. **In the civil rights complaint against MedStar Washington Hospital Center in Washington, DC, what does the obstetrician-gynecologist and fellow allege?**

   a. Administrators at the hospital told her not to talk about abortion at work.
   b. Administrators at the hospital forbade her from performing abortions at the hospital.
   c. Administrators at the hospital told her not to talk about abortion publicly.
   d. Administrators at the hospital forbade her from performing abortions anywhere.

2. **What does says Catherine J. Flynn, JD, an attorney with the law firm of Carroll McNulty Kull in Basking Ridge, NJ, say about the usefulness of audit trails in litigation?**

   a. The audit trail is more friend than foe in litigation.
   b. The audit trail usually favors the plaintiff.
   c. An audit trail is rarely of use in litigation.
   d. An audit trail is not a reliable resource.

3. **When can the Health Insurance Portability and Accountability Act become a potential conflict with a subpoena?**

   a. When the subpoena is issued by a court.
   b. When the subpoena is issued by a law enforcement agency.
   c. When the subpoena is issued by an attorney.
   d. When the subpoena is issued to a privately owned healthcare facility.

4. **What is one criticism from Gerard Gianoli, MD, FACS, a neuro-otology and skull base surgeon and a clinical associate professor at Tulane University School of Medicine in New Orleans, regarding a recent article in *The BMJ* regarding medical errors?**

   a. The study involved only 35 deaths.
   b. The study addressed only facilities that were in the United States.
   c. The study had no control group.
   d. The study data was from the 1980s.

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

HIPAA Risk Analysis Should Be Thorough And Helpful for Hospital's Compliance

A risk analysis is fundamental to any HIPAA compliance program, but conducting one effectively can be a challenge. Too often, the risk analysis is a perfunctory task that lets you check off a requirement, when it should be a valuable tool that drives the rest of your compliance efforts.

The Office for Civil Rights (OCR) studies the HIPAA risk analysis closely when investigating potential HIPAA violations, says **Kathleen D. Kenney**, JD, with the Polsinelli law firm in Chicago. She previously worked for the OCR, where she was the subject matter expert for breach notification, assisted in the administrative rulemaking process, drafted preamble language for the Omnibus Rule amending HIPAA, and actively participated on OCR's audit team. The risk analysis requirement is defined in Section 164.308(a)(1)(ii)(A) of the HIPAA standards.

"We're seeing risk analysis come up again and again in enforcement cases," Kenney says. "The big challenge for covered entities is identifying the scope of your responsibility, exactly where all your PHI [protected health information] is. It sounds like that shouldn't be so difficult, but a lot of entities struggle with it, especially when they are trying to do the analysis in the aftermath of a breach."

> "THE BIG CHALLENGE FOR COVERED ENTITIES IS IDENTIFYING THE SCOPE OF YOUR RESPONSIBILITY, EXACTLY WHERE ALL YOUR [PROTECTED HEALTH INFORMATION] IS."

The task can be challenging, because of all the many ways PHI can be stored and transmitted, Kenney says. She points to the example in which a covered entity violated HIPAA by failing to delete PHI from a photocopier before selling it. No one had realized that photocopiers can store data, so that risk wasn't included in the analysis, and, therefore, no safeguard was established.

The rapid adoption of new technology worsens the problem, Kenney says. Physicians and employees constantly are finding new devices, services, and apps that make their work more efficient, so they want to use them with PHI. The key for compliance is that you must know about the new technology and approve its use beforehand, Kenney says.

"You want to think about the risks to the data and how you are going to protect it before you allow the use of the device," she says. "Your risk analysis should help you assess the new technology and impose the appropriate limits and safeguards. OCR wants you working on the front end of this, not reacting when you find out Dr. Smith has been using a new device for six months."

Emphasizing the Scope

Providers often underestimate how broad the analysis should be, says **Leah A. Voigt**, JD, MPH, chief privacy and research integrity officer for Spectrum Health, a not-for-profit managed care healthcare organization based in Grand Rapids, MI.

"It's become clear from the Office for Civil Rights in the past couple of years that what they're looking for is far more detailed and far more comprehensive than the industry initially anticipated," Voigt says.

Voigt notes that OCR cited the failure to complete a

comprehensive risk analysis as a key problem leading to the recent $2.7 million settlement with Oregon Health & Science University (OHSU) in Portland.

"What sticks out to me as a privacy officer for a healthcare organization is that the OCR has emphasized that the risk assessment must cover all electronic PHI created or maintained by a covered entity or business associate," Voigt says. "It's that three letter word, 'all,' that I think is really important."

That expectation goes far beyond the electronic medical record, Voigt says. She advises visiting facilities to see how PHI is used in various settings and what must be included in the analysis.

"If you walk around and talk to people, you'll see that you didn't realize someone had PHI in a folder in a part of the system you didn't include," Voigt says. "This analysis is not something you can do just sitting at your desk."

Evaluate Risk and Severity

Once you have data mapped the relevant risk universe, the next step is to evaluate each risk factor and determine the likelihood and impact of these events occurring, says **Eric Dieterich**, a partner with the data privacy practice of Sunera, a cyber risk management company in Sunrise, FL.

The final phase of the risk analysis activities includes an evaluation of your current safeguards to determine the effectiveness of these activities in reducing your inherent risk rankings.

"This evaluation of safeguards is one area that organizations often fall short, increasing the risk of non-compliance with the relevant HIPAA safeguards," Dieterich says. "The HIPAA standards often require specific language to be present in internal policies and procedures, they have defined operational practices, and there is the implementation of technical safeguards, all of which can be easily overlooked."

To evaluate the effectiveness of these safeguards and identify areas of non-compliance, Dieterich says organizations should perform detailed discovery and an in-depth analysis of existing documentation, review operational practices, and evaluate relevant technologies.

"This deeper dive into the effectiveness of an organization's safeguards provides the foundation for the assigned risk mitigation of your risk analysis program, leading to a stronger compliance program and one that can stand the test of the increasing regulatory scrutiny," he says.

Give Yourself Credit

Kenney notes, however, that covered entities often do not give themselves enough credit for the safeguards they do have in place. Even if the safeguard is not ideal, perhaps because you cannot afford the best solution, you should document clearly how you are addressing the risk, she says. Otherwise, OCR could come away with a worse impression of your compliance than is warranted.

"If you can't afford encryption, note that the smartphones are password-protected and you have the ability to wipe them remotely — things like that," she says. "You want to give yourself credit where credit is due, even if there are still shortcomings from what you would do ideally."

A related problem with risk analyses is that covered entities don't act sufficiently on the information they gather, Kenney says. When risks and safeguards are identified as addressable, they must be addressed.

"OCR has said over and over in public engagements that addressable does not mean optional, but we still see entities that don't understand that," Kenney says. "You need to go through the risk analysis and determine whether the potential impact from this addressable risk is high, and, if so, what you are doing to address it. You may have to address it over a longer scope of time than you'd prefer, but you must identify the mitigation steps."

Don't Promise Too Much

Kenney also cautions against overpromising. When you identify a risk and a solution, such as encrypting phones, be careful about saying when that will be completed. If you say you're going to have the phones encrypted in six months, you may have a breach eight months later, and OCR's investigation will find that you didn't follow through on your promise.

"That puts you in a worse position than if you had been more realistic about what you could do with your resources," Kenney says. ■

SOURCES

- **Eric Dieterich**, Partner, Sunera, Sunrise, FL. Telephone: (786) 390-1490. Email: edieterich@sunera.com.
- **Kathleen D. Kenney**, JD, Polsinelli, Chicago. Telephone: (312) 463-6380. Email: kdkenney@polsinelli.com.
- **Leah A. Voigt**, JD, MPH, Chief Privacy and Research Integrity Officer, Spectrum Health, Grand Rapids, MI. Telephone: (616) 391-3998. Email: Leah.voigt@spectrumhealth.org.

First Settlement with Business Associate Shows Focus of Office for Civil Rights

For the first time, the Office for Civil Rights (OCR) has settled potential HIPAA violations with a business associate, and that settlement sheds light on how the government is assessing compliance.

Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) agreed to a monetary payment of $650,000 and a corrective action plan to settle potential HIPAA violations after the theft of a CHCS mobile device compromised the protected health information (PHI) of 412 nursing home residents. CHCS provided management and information technology services as a business associate to six skilled nursing facilities.

Although direct enforcement against business associates was authorized in the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, and detailed in The Omnibus Final Rule in 2013, this settlement is the first action under these amended laws, says **Nathan A. Kottkamp**, JD, a partner with the law firm of McGuireWoods in Richmond, VA.

The CHCS settlement indicates that relationships, in general, and business associate operations, specifically, are a growing focus of action by the OCR, Kottkamp says. In earlier action this year, two covered entities entered into settlements with OCR for failure to have business associate agreements in place. OCR also began Phase 2 audits, including business associates, in March 2016. *(For more information, see "Round 2 of Audits for HIPAA Are Focusing on Business Associates,"* Healthcare Risk Management, *June 2016, which can be accessed at http://bit.ly/1Wm2g3K.)*

The settlement amount is fairly low, which suggests that OCR is focused more on helping organizations comply than on punishing them, Kottkamp says.

"This settlement tells us that the enforcement world has changed dramatically now," Kottkamp says. "It used to be that you could say they're not going to go after business associates because there are other cases to pursue with covered entities, but no one is safe anymore. We've seen ramped up enforcement on covered entities, and now I think this signals a dramatic change in the risk for business associates."

CHCS is the first business associate to enter into a settlement, but it won't be the last. Kottkamp says it is almost certain that there will be more enforcement actions against business associates in the future.

OCR initiated its investigation on April 17, 2014, after receiving notification that CHCS had experienced a breach of PHI involving the theft of a CHCS-issued employee smartphone. The smartphone was unencrypted and was not password-protected. The information on the phone was extensive and included social security numbers, information regarding diagnosis and treatment, medical procedures, names of family members and legal guardians, and medication information.

The CHCS case underscores the risk of allowing PHI on employee smartphones, Kottkamp says. The phone in question had no security features for locking it, which allowed anyone to access the patient records. OCR's announcement stated that the egregiousness of the breach was mitigated by the fact that CHCS provides charity services to a large population of underserved patients.

"If that had been a hospital, I think we would have seen a much stiffer penalty," Kottkamp says. "This is a confirmation of what OCR has said publicly, that, at least for the moment, it is very much focused on compliance and not punishment. They're not looking to shut down somebody's business, but they want a settlement amount that gets your attention and hurts a little bit."

Tips from Corrective Plan

At the time of the incident, CHCS had no policies addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident. OCR also determined that CHCS had no risk analysis or risk management plan.

OCR will monitor CHCS for two years as part of this settlement agreement, which helps ensure that CHCS will remain compliant with its HIPAA obligations while it continues to act as a business associate. Kottkamp notes that, as is often the case, the specific terms of the corrective action plan illustrate OCR's priorities. In the CHCS corrective action plan, OCR emphasizes policies, procedures, and workforce education. *(Readers can access the corrective action plan by going online to http://bit.ly/29McWXU.)*

The CHCS case and corrective action plan can be used by covered entities to help educate their business associates about the importance of HIPAA compliance, Kottkamp says. Although the hospital is not obligated under HIPAA to ensure business associates' compliance, it is

in the covered entity's best interests to have them comply, he says. When a business associate causes a breach, it is most likely the hospital's name that will be in the headlines.

"The corrective action plan reads like OCR saying what they really care about and how to satisfy them," Kottkamp says. "You can almost go through the plan and use it as a checklist to assess your own compliance." ■

OCR: Ransomware Attack Is Usually a Data Breach

With ransomware attacks a continuing threat to hospitals and health systems, the Office for Civil Rights is warning that, in addition to all the other headaches, such incidents could be considered a data breach under HIPAA.

Ransomware attacks have been recognized by the FBI as a serious threat, and some experts predict there will be more after the February incident in which Hollywood Presbyterian Medical Center in Los Angeles paid $17,000 to hackers who took over its systems. Since then, four hospitals in California, Kentucky, and Maryland have been hit.

The Office for Civil Rights at the Department of Health and Human Services (HHS) has released new HIPAA guidance on ransomware. The new guidance points out that a ransomware attack probably means there has been a protected health information (PHI) data breach under HIPAA and says, "The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

That type of incident would trigger the notification requirements. Entities experiencing a breach of unsecured PHI must notify individuals whose information is involved in the breach, HHS says, and, in some cases, the media, unless the entity can demonstrate and document that there is a "low probability" that the information was compromised.

The guidance suggests conducting a risk analysis to identify threats and vulnerabilities to PHI and establishing a plan to mitigate or remediate those identified risks. In addition, the guidance advises taking these steps:

- Implement procedures to safeguard against malicious software.
- Train authorized users on detecting malicious software, and report such detections.
- Limit access to PHI to only those persons or software programs requiring access.
- Maintain an overall contingency plan that includes disaster recovery, emergency operations, frequent data backups, and test restorations. The guidance is available online at http://bit.ly/29zm57B. ■

Worker Fired in NFL Player Incident Sues Hospital

A secretary fired from Jackson Health System in Miami for accessing the medical record of New York Giants' football player Jason Pierre-Paul is suing Miami-Dade County's public hospital network. She claims she did not access the patient record and that the health system defamed and libeled her.

Pierre-Paul had sought treatment at Jackson Memorial after a fireworks accident over the Fourth of July weekend in 2015. A few days later, ESPN posted a photo of part of Pierre-Paul's medical record on Twitter showing that the player had had a finger amputated.

Brenda Jackson had worked for 14 years at Jackson Memorial Hospital and says in her lawsuit that hospital administrators incorrectly blamed her for the HIPAA violation and made false accusations to the media. The experience triggered nightmares, migraine headaches, and other sudden illness, according to the lawsuit, which seeks damages in excess of $15,000.

In addition to Jackson, the hospital fired a clinical staff nurse.

Jackson Health asserts that on July 21, 2015, the secretary accessed the patient's chart four times "without any necessary reason and authorization to do so."

That date is almost two weeks after the July 4 weekend when Pierre-Paul's records were leaked to ESPN, which suggests that the secretary may not have been involved with the initial leak to the media. The statement announcing the dismissal of two employees in February did not say that either was responsible for the leak to ESPN.

Pierre-Paul sued for civil damages, and the hospital announced a settlement. He is now suing ESPN. ■

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

Excessive Prescriptions Result in $17.6M Award In Compensatory and Punitive Damages

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

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

Rebeka Rioth*, 2017 JD Candidate*
Pepperdine University School of Law
Malibu, CA

News: In 2008, a 45-year-old man's primary care physician began prescribing powerful and highly addictive pain pills for lower-back pain. The pain pills, known as opioids, are prescribed at alarming levels for millions of patients in the United States, which results in frequent addiction and serious side effects. From 2008 to 2012, the man's doctor increased the dose of opioids dramatically, which caused depression, loss of employment, and, ultimately, the need for entering a drug rehabilitation center for the treatment of opioid addiction. The man and his wife filed a medical malpractice lawsuit against the primary care physician and the hospital for the negligent and reckless act of prescribing opioids at dangerous levels, and they won $17.6 million in damages.

> ... OPIOIDS ... ARE PRESCRIBED AT ALARMING LEVELS FOR MILLIONS OF PATIENTS IN THE UNITED STATES.

Background: In 2008, a 45-year-old man went to his primary care physician complaining of lower back pain. The man's doctor immediately began prescribing opioids, highly addictive narcotic pain medications, which are commonly used to treat moderate to severe pain that may not respond well to other pain medications.

From 2008 to 2012, the doctor continued to prescribe the man increasingly higher doses of opioids for back pain. Despite the fact that the man's back pain did not improve, the doctor continued to prescribe pain pills. At one point, the man was taking multiple types of opioids, including Vicodin and OxyContin. During the four-year period, the man was prescribed 37,000 pain pills, with an average daily dose that rose from 49 mg to 1555 mg.

The cumulative effect of the pain pills resulted in the man's inability to continue his job as a mechanical maintenance worker, estrangement from his wife and daughter, and severe depression. Although the man left the care of his primary physician some time in 2012, he became addicted to the prescribed pain medications and eventually entered a drug rehabilitation center to obtain treatment for his addiction.

The man and his wife eventually sued the man's primary care doctor as well as the hospital, and they alleged that the doctor and the hospital were negligent in prescribing a massive quantity of highly addictive pain medications for back pain. Attorneys for the hospital and doctor argued that while opioid prescriptions of more than 100 mg per day render a patient at risk for serious side effects and addictive behaviors, the man ultimately was responsible for his addiction and the side effects that accompanied the pain pills.

After a seven-day jury trial, the jury returned a verdict in favor of the man and found that the doctor and the hospital were guilty of medical malpractice in the negligent administration of massive doses of opioids. Although the jury initially awarded the man and his wife $17.6 million in damages, the award will be reduced because the jury also found that the man was partially responsible for the addiction that resulted from the initial dose of opioids in

2008. The award also is significant in that $15 million of the award was for punitive damages, which are intended to punish the defendant rather than compensate the plaintiff.

What this means for you: This is a landmark case in the current opioid abuse epidemic in the United States. It was an undisputed fact during the trial that opioids are overprescribed in the United States medical system at dangerous levels and that primary care physicians, therefore, have a duty to closely monitor the administration of these pain medications.

However, and somewhat at tension with this prior statement, there has been additional pressure put on physicians and hospitals by regulatory and accreditation agencies such as The Joint Commission and CMS (previously) to manage pain as part of patient rights. This focus caused a reversal in the usual reluctance of physicians to prescribe opioids for fear of their addictive properties and resulted in the now-common practice of ordering them as the first line of defense against even mild pain. These drugs work well for the opiate naïve, but they require continual dose increases to maintain their effectiveness as patients' bodies become tolerant. Patients with chronic pain lasting years require doses that far exceed drug manufacturer, FDA, or CDC recommendations.

Expert physicians for the man testified that many primary care physicians are under the misperception that drug toxicity, or harmful reactions from opioid overdoses, can be avoided by slowly adjusting the dose of opioids for non-cancer pain upward over time. However, it is this incorrect view that has led to the epidemic of dangerously high doses of opioids in patients with simple maladies such as back pain. It is also relevant to note that not only did the jury, in this case, find the primary care doctor in breach of the proper standard of medical care, but it also held the hospital responsible for failing to monitor the type and level of pain medications that the doctor was administering over a prolonged period of time. Physicians struggling to manage patients with chronic pain can and should consult with their colleagues who specialize in pain management, an expanding field of medical practice, as well as provide referrals for non-traditional medical interventions such as acupuncture, holistic, and/or herbal modalities.

Additionally, the outcome of this case was dependent not only on the use of expert physician testimony, but also on evidence from the CDC, which regularly issues guidelines for the appropriate administration of medications. Attorneys for the man relied on a recent CDC guideline that cautioned against an average daily dose of more than 100 mg of opioids. This piece of evidence was successful in establishing the appropriate standard of medical care, which ultimately would reveal the high degree of recklessness on the part of the doctor and hospital for prescribing opioids on a daily average of 1555 mg toward the end of the four-year period. ■

REFERENCE

St. Louis County Circuit Court, Missouri, Case No. 1422-CC01258 (June 28, 2016).

Failure to Recognize Post-surgery Problem Caused Internal Bleeding Yields $4.3M Verdict

News: In 2010, a 57-year-old woman was admitted to a hospital to undergo surgery to permanently stitch her stomach into the correct anatomical position after a hiatal hernia caused her stomach to partially invade her chest cavity. When the woman's blood pressure dropped tremendously post-surgery, the medical team failed to identify the problem, and they mistreated it. At trial, the jury returned a verdict in favor of the woman in the amount of $4.3 million, and it found that the hospital and the anesthesia group violated the appropriate standard of care and negligently caused the woman's death.

Background: On Oct. 8, 2010, a 57-year-old woman was admitted to a hospital to undergo laparoscopic surgery to repair a hiatal hernia. The hiatal hernia had caused the woman's stomach to bulge upward and partially invade her chest cavity. The doctors intended to perform a procedure known as a Nissen fundoplication to permanently stitch the woman's stomach back into the correct anatomical position.

After surgery, the woman was transported to the hospital's postanesthesia care unit, where the on-call nurse noticed that the woman's blood pressure was dropping at an increasing rate. Following an 83-minute surgery, the woman's blood pressure was 106/49. Ten

minutes later, her blood pressure had dropped to 75/45.

The on-call nurse called the anesthesiologist in charge of the woman's care, who ordered the intravenous administration of ephedrine, a vasopressor medication used to treat low blood pressure. After no improvement, the anesthesiologist was called a second time and gave the nurse an order for another dose of ephedrine. Once the woman's blood pressure dropped to 63/34, the anesthesiologist was contacted a third time, after which he ordered two additional vasopressors, vasopressin and then Neo-Synephrine, in an attempt to raise the woman's blood pressure.

At this time, the general surgeon who performed the Nissen fundoplication briefly checked on the woman and, although aware of the woman's low blood pressure, did not perform a surgical consultation or order any tests. After there was no improvement in the woman's blood pressure, the on-call surgeon ordered a complete blood count, a comprehensive metabolic panel, and chest X-rays. However, the woman soon became unresponsive, and doctors performed a second, emergency surgery in which they found a pulsatile arterial bleed that caused her entire abdomen to fill with blood.

Although doctors were able to stop the bleed, the massive blood loss caused the development of a disseminated intravascular coagulation (DIC), which is a condition in which a patient begins to spontaneously bleed from multiple locations. As a result, the woman was placed on life support after surgery. The following day, she was taken off life support and pronounced dead.

The woman's daughter filed a wrongful death lawsuit against the anesthesia group that employed the anesthesiologist, the hospital, and the clinic that employed the doctors who performed the laparoscopic surgery. The plaintiff's attorneys argued that the anesthesiologist should have suspected internal bleeding after the woman's low blood pressure did not improve following the administration of ephedrine.

They further argued that this failure to consider the possibility of an internal bleed caused the woman to reach the point of no return once she became unresponsive in the postanesthesia care unit. The attorneys asserted that, had the general surgeon or anesthesiologist detected an internal bleed earlier, the woman would have returned to the operating room sooner to address the bleed and her death ultimately would have been prevented.

Attorneys for the hospital and anesthesia group argued that shortly after the woman's Nissen fundoplication, she experienced a spasm in one of her arteries that had been cauterized in surgery, and it was this spasm that caused the internal bleed. Furthermore, they argued that even if the anesthesiologist had ordered a complete blood count sooner, the test would not have been determinative of any internal bleeding. They also believed that because it is normal for patients who undergo anesthesia to experience low blood pressure, the woman's low blood pressure post-surgery was not indicative of an internal bleed.

Following trial, a jury returned a verdict in favor of the plaintiff in the amount of $4.3 million. The jury found that the hospital and the anesthesia group, which employed the anesthesiologist in charge of the woman's care, violated the appropriate standard of care and negligently caused the woman's death. Although the anesthesia group appealed the verdict, an appellate court affirmed the trial court's ruling.

What this means for you: This case illustrates the importance of patient postoperative care. Although there may be no obvious complications occurring during a surgical procedure itself, a patient is still at risk of postoperative complications. Consequently, it is imperative that healthcare professionals employ practices and methods that can efficiently diagnose a condition once the patient begins to show any abnormal signs or symptoms or significant changes in baseline vital signs, such as pulse, respiratory rate, and blood pressure, all established during the preoperative assessment required before surgery begins. A blood pressure of 63/34 in an otherwise healthy person is indicative of a massive hemorrhage, and emergency procedures should have been activated, including immediate callback of the surgical team, initiation of a massive transfusion protocol, and a rapid response or code blue call within the facility.

Unfortunately, in this case, the anesthesiologist continued to administer various medications for treating low blood pressure without physically examining the woman, ordering any tests, or considering any underlying causes of the low blood pressure, such as internal bleeding. This response is especially significant given the fact that the Nissen fundoplication required the repeated cauterization of the woman's arteries, which substantially increased the likelihood of the woman developing an internal bleed post-surgery. Had the woman been examined by the surgeon or anesthesiologist, a hot, rigid abdomen would have been

detected, which would have indicated the bleeding taking place below.

This case also exemplifies how quickly a patient's condition can go from stable to critical and, in turn, how healthcare professionals can be held responsible for the decisions made during these crucial moments. In this case, the attorneys for the woman were successful in convincing a jury that postoperative tests, such as a complete blood count, a comprehensive metabolic panel, and chest X-rays, should have been ordered soon after the woman's blood pressure began to drop. The implication of this conclusion is that the jury was unconvinced that the anesthesiologist's method of ordering three medications without examining the woman in person met the standard of care in this case.

The outcome of this case also was heavily dependent on the use of medical experts on both sides. Three medical experts testified on behalf of the woman to establish the appropriate standard of care for patients who undergo Nissen fundoplications. One of the experts testified that the woman's blood pressure was extremely low and that the anesthesiologist should have considered internal bleeding as a possible cause after the woman failed to respond to the administration of the first medication, ephedrine. Additionally, the expert believed that, had the anesthesiologist notified the general surgeon sooner of the woman's unimproved condition, this may have resulted in an earlier return to the operating room and prevented the woman's death.

Expert testimony often is critical in medical malpractice cases, and it is important for clients in such cases to quickly identify and secure the assistance of qualified experts. Having an expert on board early in the case is important for shaping the approach to the entire case and, thus, justifies the expense of early involvement. Waiting until the end of the case to secure an expert, and then find out that the case has not been properly developed to suit the expert's needs, is "penny wise and pound foolish."

There are several methods for finding expert witnesses. Often, attorneys who specialize in medical malpractice cases have a stable of experts they like to use, but in such situations (when someone regularly gives expert testimony), it is important to try to find someone who maintains a balanced portfolio of plaintiff side and defense side cases. A seasoned expert with a balanced portfolio of work will maintain the aura of independence better than someone who handles cases only for one side or the other, which conveys the impression of a "hired gun" who will say whatever a party needs, thus undermining the credibility and value of the opinion.

EXPERT TESTIMONY OFTEN IS CRITICAL IN MEDICAL MALPRACTICE CASES ...

When counsel doesn't immediately have in mind a couple of candidates to serve as expert witnesses, he or she usually will start a search by asking colleagues in the legal community for recommendations, but if that does not yield any strong prospects, it will become necessary to commence a search from scratch. Depending on the subject matter, other doctors practicing in a given area are obvious candidates, as are academics. Some counsel are cautious, if not simply disinclined, to work with potential experts who never have served, but with the proper introduction to the litigation process and some extra attention to training in effective oral presentation, even a new expert can be a very powerful witness. The most important aspects of the process are complete mastery of the subject matter and the ability to convey the opinion and the reasoning behind the opinion in a simple and straightforward manner to the finder of fact, whether that be a jury or a judge.

All experts need to carve out time to work with counsel and with the client to prepare for testimony in a specific case. Ironically, it is sometimes the most seasoned experts who are the most difficult to work with in this regard because they may believe erroneously that they don't need to prepare vigorously because they've seen it all before. However, every medical malpractice case will have its own unique facts, medical records, and other twists, and an expert who is unprepared to apply those to his or her general base of knowledge will be much less persuasive than one who is sharp with the case. There is also the risk that an expert who has not sufficiently connected his or her body of knowledge to the actual facts of the case may be precluded from testifying as a result of a pretrial motion called a motion *in limine.* Therefore, it is critical for the client and his or her counsel to make sure the expert devotes sufficient time to preparing for the specific case. ■

REFERENCE

DeKalb County Circuit Court, Illinois, Case No. 10-L-113 (June 20, 2016).