HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE SINCE 1979

INSIDE



RELIAS MEDIA

MARCH 2020 Vol. 42, No. 3; p. 25-36

# Boards of Directors on Notice With Recent Caremark Decisions

Members of healthcare boards of directors may be at significantly higher risk of personal liability and lawsuits alleging failure in the duty to monitor. Risk managers should act now to educate their corporate boards and review compliance with the obligations that could lead to litigation.

Two recent Delaware court decisions addressed a corporate board's Caremark duty to monitor, explains **Roger D. Strode**, JD, partner with Foley & Lardner in Chicago. The Caremark duty is derived from *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996), a civil action concerning a director's duty of care, Strode says.

> "THESE COURTS ARE INDICATING THAT THE OUTLOOK ON CAREMARK IS CHANGING IN A SIGNIFICANT WAY, AND DIRECTORS FACE A GREATER RISK OF LIABILITY THAN THEY MIGHT HAVE IN THE PAST."

The *Caremark* decision established that corporate directors breached their oversight duty when they knew or should have known that violations of the law were occurring, took no steps to prevent or remedy the situation, and that failure resulted in the losses alleged by the complainant.

In one of the more recent decisions, on Oct.1, 2019, the Delaware Court of Chancery issued an opinion in *In re Clovis Oncology, Inc. Derivative Litigation*. That case involved stockholder plaintiffs claiming the board of directors failed to monitor the accuracy of the company's clinical trial protocols and compliance with regulatory mandates. They further claimed the company misled the market regarding



**Financial Disclosure:** Author **Greg Freeman**, Editor **Jill Drachenberg**, Editor **Jonathan Springston**, Editorial Group Manager **Leslie Coplin**, Accreditations Manager **Amy Johnson, MSN, RN, CPN**, 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. Consulting Editor **Arnold Mackles**, MD, MBA, LHRM, discloses that he is an author and advisory board member for The Sullivan Group and that he is owner, stockholder, presenter, author, and consultant for Innovative Healthcare Compliance Group.

HEALTHCARE RISK MANAGEMENT™

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

**GST Registration Number: R128870672**

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

**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@reliasmedia.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.

**ACCREDITATION:** Relias 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 LLC is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians. Relias LLC designates this enduring material for a maximum of 1.5 *AMA PRA Category 1 Credits*™. Physicians should claim only credit commensurate with the extent of their participation in 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
**EDITORIAL GROUP MANAGER:** Leslie Coplin
**ACCREDITATIONS MANAGER:** Amy M. Johnson, MSN, RN, CPN



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

the efficacy and likely FDA approval of a drug under development.

The court denied a motion to dismiss the Caremark claim, saying the board's alleged failure to monitor established systems in the face of "red flags" was problematic because *Marchand* requires that "when a company operates in an environment where externally imposed regulations govern its 'mission critical' operations, the board's oversight function must be more rigorously exercised."

In *Marchand v. Barnhill*, 2019 WL 2509617 (Del. June 18, 2019), the Delaware Supreme Court allowed a lawsuit to proceed against directors of an ice cream manufacturer. Blue Bell Creameries was involved in a listeria outbreak in early 2015 that killed three people, forced the company to recall all of its products, shut down production, and lay off more than one-third of its workforce. A shareholder sued the company directors for failure of oversight regarding food safety and compliance matters.

The Delaware Supreme Court ruled it was reasonable to infer that the Blue Bell directors consciously failed "to attempt to assure a reasonable information and reporting system existed," allowing the Caremark claim to continue.

The effects of the rulings may be felt across the country because Delaware law is influential for other states, Strode explains. Most publicly traded companies are organized in Delaware because the state has the most formalized statutes and greatest body of case law regarding corporations and business organization, he notes.

"Courts and corporate lawyers will look to Delaware law to guide them on issues related to board duty, fiduciary duty, duties of oversight, care, and loyalty. Delaware often is at the tip of the spear when it comes to issues like this," he says. "Their formalized structure on corporations is where other states look for guidance and case law precedents, even though it is not binding precedents in other states."

The two decisions mean that corporate boards should be much more wary of violating Caremark requirements, Strode says.

"These courts are indicating that the outlook on Caremark is changing in a significant way, and directors face a greater risk of liability than they might have in the past, which means they may need to change how they do business," Strode says. "The duty to monitor has been well established but boards have had the comfort of knowing that the bar was fairly high for being held liable. With these decisions, there is reason to think that is changing."

## EXECUTIVE SUMMARY

Two recent court rulings indicate courts may extend a corporate board's duty to monitor further than the previous norm. Healthcare corporate directors could be at an increased risk of shareholder lawsuits and personal liability.

- The cases are from Delaware, where rulings are influential on other states.
- The bar has been lowered for director accountability.
- Healthcare organizations should review their risk assessment and compliance programs.

Although the two decisions did not involve healthcare entities, Strode says there is a direct line of sight legally to health systems, hospitals, and other providers, because they have similarly "monoline" functions of providing quality clinical care in a highly regulated environment. The recent decisions emphasized that the companies had monoline functions — developing drugs and making ice cream — that a board could oversee without its focus splintering across multiple lines of business.

The court rulings also noted the highly regulated environments of drug development and commercial food production, where FDA regulations apply. Strode says it is reasonable to think the courts would see the same scenario with regulations from the Centers for Medicare & Medicaid Services, plus state departments of health.

The risk exists even for not-for-profit healthcare organizations without shareholders, Strode notes. Bondholders can sue if their investments are damaged. State attorneys general could assert charitable doctrine authority to adopt the legal posture of a shareholder, he explains.

"Before *Clovis* and *Marchand*, a Caremark claim was a tall order for the claimant. Bringing a case under Caremark was no guarantee of success, and in fact was often a real long shot," Strode says. "You weren't going to get a ruling in favor of a claim for director liability unless you could prove sustained or systemic failure of oversight. The bar has been lowered, and I think we may see more directors held liable."

The courts are making clear boards must actively monitor compliance. In *Clovis*, Strode says the court's decision means lack of action can be a basis of a failure of the duty of oversight. In *Marchand*, he explains, the court held the plaintiffs alleged sufficient facts to conclude that the Blue Bell board failed to implement any system to monitor food safety risk. The *Marchand* court said the "utter failure to attempt to assure a reasonable information reporting system exists is an act of bad faith and breach of a duty of loyalty."

SMALLER HEALTHCARE ORGANIZATIONS MAY FACE MORE RISK IN THIS AREA SIMPLY BECAUSE THEY DO NOT HAVE ADEQUATE RESOURCES TO PROPERLY MEET THE CAREMARK REQUIREMENTS.

Both points could prove relevant in a healthcare entity's failure to ensure patient safety, Strode notes. Boards for healthcare organizations are obligated to use risk-monitoring systems and ensure any identified issues are addressed. Any policies, procedures, and protocols implemented under those risk systems must be followed, he says.

"The organization risk manager and the board, with the support of counsel, should review internal and external risks and compliance on a regular schedule, at least twice a year if not more often," Strode says. "There should be discussion at board meetings that are specifically devoted to these risk assessments and compliance obligations."

The *Marchand* ruling also showed the need for an appropriate committee structure for risk assessment and compliance, Strode says. The court endorsed the idea of a committee that provides general compliance oversight.

Corporate information reporting systems also were relevant to the recent decisions. The courts indicated the systems should provide the board with information it can use to reach informed judgments on matters of safety and compliance, Strode says.

"In both *Clovis* and *Marchand*, part of what got them into trouble was that their boards could not rely on board agendas and minutes to show they were aware of important issues and addressing them adequately," Strode explains. "The documentation was insufficient to show that they were receiving accurate, timely information on these issues and that they were taking the steps necessary to reach the Caremark threshold. Like everything else in healthcare, documentation can make or break your defense."

Smaller healthcare organizations may face more risk in this area simply because they do not have adequate resources to properly meet the Caremark requirements, Strode says.

"They may not have the infrastructure or sophistication at the board level, or the internal knowledge of how to put in place the right processes, everything they need to comply with the duty of oversight," Strode says. "Like everything with risk management, when you have less money and resources, you're going to be at a higher degree of risk." ■

## SOURCE


- **Roger D. Strode**, JD, Partner, Foley & Lardner, Chicago. Phone: (312) 832-4565. Email: rstrode@foley.com.

# Develop Plan for Responding to Adverse Events

Adverse events happen without warning, yet they require a carefully planned response to minimize damage and facilitate the most effective follow-up investigation. Facilities should plan now for how to respond to an unexpected death, a serious accident, or potential malpractice.

It is critical to prepare an adverse event plan so that the response is not cobbled together in the heat of the moment, when emotions are running high, says **Susan L. Montminy**, MPA, RN, BSN, CPHRM, CPPS, TeamSTEPPS Master Trainer, manager in risk management with Coverys, a liability insurer in East Greenwich, RI.

The plan should include rapid assembly of a multidisciplinary adverse event response team when the situation warrants, she says. The event will dictate who should be involved in the response, but typically the team will include clinical leaders and administrators, and it may include biomedical engineers, facilities management, security, or others.

"It begins at the top with a commitment from leadership that support and guidance is available 24 hours a day, when a single clinician is faced with an adverse event," Montminy says. "This is key to reducing potential fallout and additional risk. It's not enough to have this great team of people ready to respond during regular business hours, because that's not the only time adverse events occur."

Risk managers will play key roles in any adverse event response. Montminy says they should be "calm voices on the other end of the phone line as a crisis is unfolding." They should quickly ask the right questions, drawing out the information most necessary in the initial moments to determine the scale of the problem and the appropriate response, she says.

"Fear is always present. You must factor that into your plan, and be ready to acknowledge and address the emotions that you are going to encounter in these situations," she says.

## Many Different Events

Because adverse events can take many forms, risk managers should develop more than one type of response plan, says **Heather Macre**, JD, director with Fennemore Craig in Phoenix. A good plan starts with a risk assessment, steps to reduce or mitigate those risks, and staff education. Plans should be flexible and consider the particular needs of the practice, its patients, and practitioners, Macre says.

"The biggest thing is to have a plan in place and to update it periodically. Create a culture of accountability," she explains. "You should also make sure that everyone knows the basics of the plan and how to execute it, as well as where to find a copy of the plan. There should be regular and specific training as to what to do in emergent situations of different types."

The immediate response should focus on the safety of patients and staff, Macre says. Certain events, such as ransomware attacks that affect patient records or systems, require reporting. The quicker an incident is reported, the better the outcome in many cases.

Longer-term goals should include crisis communications to reassure patients and staff, a review of how a plan was implemented, and what can be improved, Macre notes.

"There are lots of pitfalls, but the most common is either not having an adequate plan, failing to update a plan, or not educating staff as to the contents of a plan," she says. "Evidence preservation is crucial. All computer systems should be backed up, and offsite backup is extremely useful if there is a fire or natural disaster."

## Document Carefully

Safely document as much as possible at the time of occurrence, she says. Take photos, write down thoughts and observations, and interview witnesses as appropriate, she advises.

"Certain events, such as an outbreak of infectious disease or a cyberattack, require both state and local reporting. Consult counsel immediately as they can help you report the incident to the right

### EXECUTIVE SUMMARY

It is essential for healthcare organizations to maintain a response plan for adverse events. There are certain steps and actions that must take place for an effective response.

- Develop adverse event response teams.
- Plan for a wide range of adverse events.
- Preserve documentation and other evidence.

people," Macre says. "Also, do not forget to call the police or FBI as needed. I have seen incidents where the authorities were not called until after the event, which hampers investigations."

The foundation of any plan for responding to an adverse hospital event must be the need for a rapid response, says **David Richman**, JD, partner with Rivkin Radler in Uniondale, NY. Risk management should visit the scene of the incident — the floor, the procedure room, ICU, radiology department — prepared to conduct what amounts to a triage of the incident, Richman says. In that regard, it is advisable for the risk manager to create a checklist that should be implemented immediately after notification of an incident, Richman says. *(See sidebar on the right for Richman's suggested checklist.)*

The longer-term response should require maintenance of all records related to the incident in a secure location to ensure the records remain unchanged from the date of the incident, Richman says. Similarly, any equipment involved should be kept in a safe and secure location until any state investigation is complete or any litigation that may arise has been resolved.

Richman stresses that no member of management or anyone involved with the incident can be permitted to "manage" the situation by coercing people, encouraging a unified story, or pressing staff to alter recollections of events.

"Similarly, staff should not be encouraged to add or alter notes in the chart in order to offer a description of events that may better serve the facility's defense. Additionally, should equipment be involved, it should not be subject to repair or alteration in response to the incident," Richman says. "Such conduct, conduct intended to change the narrative, will be deemed a cover-up and will be far more difficult for the facility to defend than defending the truth of what occurred."

It is important to note that adverse event responses include a wide range of events, and planned responses will vary widely, says **Kerin Torpey Bashaw**, MPH, BSN, RN, senior

## Checklist for Responding to Adverse Events

Risk managers should create a checklist for responding to adverse events to ensure the most effective response in a potentially stressful and hectic environment, says **David Richman**, JD, partner with Rivkin Radler in Uniondale, NY.

Richman says the list should include these elements:

- Notify hospital or facility management as soon as possible.
- Inform either in-house or outside counsel, or both. A determination should be made whether counsel should be involved with the early stages of incident investigation.
- Secure the chart as soon as possible. Risk management should take possession of the written chart (if one exists) immediately, and also should lock down the EMR to prevent any changes to the existing chart.
- Risk management should identify and document all involved personnel, from each category of staff, including nonmedical technical staff assigned by equipment manufacturers who have representatives present for the treatment at issue.
- Conduct interviews of all staff and document all witness statements.
- If equipment is involved as a possible cause or contributor to the event, it should be taken out of service and placed in a safe location. No one should be permitted to repair or in any way alter the equipment. Locate and secure all paperwork related to the device, including but not limited to purchase and repair records.
- Depending on the nature of the incident, the state should be informed as soon as possible of an incident to ensure everything is reported. For example, the New York State Department of Health requires that it be informed within 24 hours of an adverse event, or when the hospital reasonably believes that an adverse event has occurred. The definition of adverse events may vary from state to state but will be wide-ranging.
- Social workers should be contacted to serve as intermediaries with the family, and be available to the family as soon as possible to answer questions, or assure family and friends that any questions will be answered subject to coordination with facility management and its counsel.
- If the facility has a public relations department, members of that staff should be brought into the discussion in the event publicity is generated and/or it becomes necessary that a public statement be made. ■

vice president in the Department of Patient Safety & Risk Management with The Doctors Company, a liability insurer based in Napa, CA. An adverse event is an incident that has caused or could have caused harm to a patient because of medical care, she says.

There are minor variations in classification between organizations. Guidance for immediate and long-term response to adverse events comes from a variety of sources, including the Department of Health and Human Services through the Conditions of Participation for Medicare and Medicaid, accreditation bodies such as The Joint Commission, and state departments of public health, she notes.

Organizations are required to create policies and procedures that meet requirements for their state and/or accrediting body. There are some requirements for mandatory reporting to the state and organization with specific time frames, Torpey Bashaw says. If mandated reporting does not occur, some states will impose daily financial fines on the organization for failure to report an event within the time frame, she notes.

As 24 states have enacted mandatory requirements for reporting adverse events meeting specific criteria, a clear organizational policy is required to quickly identify and respond to serious clinical risk and adverse events, Torpey Bashaw says.

"All areas that provide clinical care need to have policies and procedures clearly outlining the response, escalation, and resolution process for adverse events. Plans also should include a standard process and timelines to complete an investigation and/or root cause analysis for the event, presenting findings to leadership for resolution and monitoring," she says. "Plans also should include provisions for tracking and trending data related to incidents and events to make sure corrective action plans are effective and new risks do not emerge."

Individuals at all levels of the organization should be familiar with the process for identification and reporting or escalating adverse events up the chain of command until the event has been stabilized or resolved, Torpey Bashaw says. Staff are responsible for continually escalating up the chain of command until stabilization and/or resolution has occurred, she says.

Significant or never events should be immediately reported verbally up the administrative chain for instant response to limit any further harm and to inform the patient and family of the event facts, she says. The risk manager should be notified verbally as soon as possible, and support the communication process with the patient.

Preservation of evidence and documentation should occur right away, but Torpey Bashaw notes this often does not happen when individuals are unaware of the requirement to preserve and lock down space and documentation to protect facts that will serve in the root cause analysis.

"Supplies, equipment, and space should not be touched after an event until an administrative leader or risk manager comes to the space to assess, sequester, and preserve appropriate items and document. Paper and nondigital documents should be taken into custody and copied to preserve original integrity," she says. "Digital documents are timestamped and can be tracked using an audit feature. All of this information should be used during the comprehensive investigation." ■

## SOURCES


- **Heather Macre**, JD, Director, Fennemore Craig, Phoenix. Phone: (602) 916-5396. Email: hmacre@fclaw.com.
- **Susan L. Montminy**, MPA, RN, BSN, CPHRM, CPPS, TeamSTEPPS Master Trainer, Manager, Risk Management, Coverys, East Greenwich, RI. Phone: (800) 225-6168. Email: coverys@pancomm.com.
- **David Richman**, JD, Partner, Rivkin Radler, Uniondale, NY. Phone: (516) 357-3120. Email: david.richman@rivkin.com.
- **Kerin Torpey Bashaw**, MPH, BSN, RN, Senior Vice President, Department of Patient Safety & Risk Management, The Doctors Company, Napa, CA. Phone: (707) 226-0291. Email: kerin.bashaw@thedoctors.com.

# Include Communications in Adverse Event Plans

When planning to respond effectively to adverse events, it is important to include a crisis communication plan, says **Janey Bishoff**, an expert in crisis management and crisis management planning.

Bishoff taught corporate crisis management at Boston University, and now is owner of Bishoff Communications in Needham, MA. She says a crisis communication plan is essential to protect the organization's reputation.

"It is a critical risk management component, and the best way to assure leadership and key management that everyone in the organization knows what to do and what not to do when any adverse event occurs," she says. "The plan should not be a hefty notebook that sits on a shelf, but rather a series of checklists and charts that are readily available and can be easily consulted for quick referral in any urgent, fast-moving situation."

A key part of the plan is a designated crisis team including members for each defined functional area of the organization, Bishoff says. There must be backups assigned for each functional area of the team, she explains, because crises rarely occur during the normal workday when everyone is in the area and on site.

"The backups on the crisis team are critical to ensure that the organization is prepared to respond, even when key leaders are on a plane or halfway around the world," Bishoff says. "For some healthcare organizations, some members of the crisis team may only be designated for certain types of situations. For example, if the situation does not involve patients and clinical staff, some key clinical members of the crisis team may not be needed."

## Know the Roles

For the plan to be effective, everyone on the crisis team must be intimately familiar with the roles and prescribed processes, she says. The designated spokespeople for the organization must undergo media training. Often, the spokesperson in a crisis must be a top leader, not the "everyday" spokesperson, Bishoff says.

"It is essential that those leaders undergo rigorous media training before any adverse event occurs," she says. "Everyone in the organization should know that there is a crisis team, that there are designated spokespeople, and that no one else should ever speak on behalf of the organization."

Communication in the world outside an organization is instantaneous, so communication inside should be, too, she says. The crisis team must be ready to meet, in person or virtually, to respond and take on their responsibilities on a moment's notice.

The immediate response must acknowledge the situation, Bishoff says. This does not mean that the organization needs to assume responsibility for what happened, nor does it mean that the response must include information about how leadership will fix the situation.

"It simply means that the leadership understands that there is a negative situation, and is taking appropriate steps to investigate and find out what happened," she says. "Ideally, the response will include a promise to inform stakeholders once the investigation has occurred."

The immediate response may need to communicate instructions to certain stakeholders, Bishoff says. It may need to inform stakeholders to prevent harm or worsening of the situation. For example, because of certain situations, leadership may need to tell visitors not to come to the hospital, or tell the public not to come to the hospital's ED for the next 24 hours, she explains.

"The immediate response must demonstrate compassion — even if the organization is not responsible, and even if the organization is going to have to prove that it is not responsible," Bishoff says. "To inspire confidence among stakeholders, the immediate response must communicate that the leadership is in charge and intends to find out what happened, how it happened, and why it happened. To the extent possible, the immediate response should demonstrate that the organization is committed to be as transparent as possible."

## Elements of a Plan

Bishoff recommends these essential elements of a crisis communication plan:

• **Crisis simulation.** The best way for the team to prepare is to conduct a crisis simulation (at least one per year), just as clinicians often run drills for emergencies. At minimum, a tabletop simulation should be conducted.

• **Holding statements in the drawer.** A set of basic "holding" statements should be developed and readily available to be customized and issued on a moment's notice. Such statements should be written before any adverse event occurs to ensure

consistency with the organization's key messaging, and reinforce those messages.

• **Media/social media monitoring.** Develop a system for comprehensive media monitoring to be apprised of news media coverage and stakeholder reaction.

• **Continued crisis team vigilance.** Once the initial hours of the situation are over, it often is too easy to resume normalcy and neglect further "clean-up" responsibilities, such as follow-up communications, that are needed to protect reputation long term.

• **Dark website page.** Ideally, the organization should maintain a dark website page that is not accessible by the general public, and not active until needed. This website can be used to provide information for various stakeholders about the crisis.

There are multiple pitfalls to avoid in crisis communication, Bishoff says. The first is not responding in a timely manner, or not responding at all. Responding publicly in a crisis today is essential and must be immediate, she says.

"Failing to respond is seen as suspect, as if the organization has something to hide or does not care. Even though fact-gathering in a crisis is critical and often takes time, waiting too long to respond may diminish trust and negatively impact reputation long term," she says. "Most importantly, by not responding in a timely way, the organization cedes control of the message. In these situations, news media and social media can quickly define a negative message, which will be difficult, if not impossible, to overcome."

Another pitfall is not showing compassion. Even if the facts are sketchy, and even if litigation is likely to occur that will establish fault or responsibility, the initial response must demonstrate compassion for any individuals who were hurt, taken ill, or died, Bishoff says.

"This is where it is critical to have an experienced crisis manager participate in guiding the response since attorneys, in an effort to protect the organization in future litigation, often advocate that the organization say nothing," Bishoff says. "In-house communications professionals, and even savvy, but less experienced external communications consultants, are not used to, nor should be put in a position to, argue with the organization's legal counsel." ■

### SOURCE


- **Janey Bishoff**, Bishoff Communications, Needham, MA. Phone: (617) 573-0076. Email: jbishoff@bishoffcommunications.com.


# Choose Outside Counsel Carefully; Avoid Common Mistakes

When risk managers are involved in selecting outside counsel for the hospital or health system, the task can seem daunting. Or, it can seem deceptively simple because every lawyer in town wants the business.

Choosing the right counsel involves considering a multitude of factors, including fees, availability, experience, size of the firm, and even whether it seems like a good fit culturally.

When choosing outside counsel, there is a myth that bigger is better, says **Edward T. Waters**, JD, managing partner with Feldesman Tucker Leifer Fidell in Washington, DC.

"That is just not true. There are many boutique firms like ours with many experts on the arcana of Medicare, Medicaid, and other federal healthcare programs such as federally qualified health centers, Ryan White HIV/AIDS Program, and the recent array of opioid funding," he says. "What you get with a boutique is an expert who will pay attention to your problem, and not heavily staff the matter with the attendant high cost."

Finding an expert in your subject matter also can be problematic, Waters says. The American healthcare system is extraordinarily complex, and lawyers, like physicians, specialize. That means risk managers must take the time to understand the firm's depth of knowledge on particular issues, he says.

"Also consider: is the attorney or firm responsive? Are they problem-solvers? Do they make sense? Can they communicate their advice in a clear and understandable way? Do you see working closely with this attorney or attorneys as a positive or a negative?," Waters says. "People, organizations, hospitals come to a lawyer for leadership, and they need help navigating through their issue or issues."

Clear, understandable analysis and proposed solutions is key, as is working together to solve the problem, Waters says.

"If the attorney isn't clear, is hard to work with, doesn't keep you up to date, or fails to respond to requests in

a timely way, it is time to find a new lawyer," he says. *(See the story on page 34 for a list of factors to consider in choosing outside counsel.)*

## Experience Matters

It is important to choose an experienced lawyer with demonstrated subject matter expertise, and a reputation and presence in his or her field, says **Wendi Campbell Rogaliner**, JD, partner with Bradley Arant Boult Cummings in Dallas. However, it also is important to dig a little deeper, and to interview potential candidates to make an informed choice, she says.

Additional factors to consider in the interview process include the ability of the attorney's law firm to staff the matter appropriately. For example, a solo lawyer with undeniable expertise and an impeccable reputation might not be able to efficiently staff a large-scale project, she explains. Appropriate staffing drives efficiency and fees. Healthcare organizations do not want to pay partner-level rates for associate and/or paralegal work, she adds.

Other topics for discussion in the interview should include the lawyer's ability to create, communicate, and justify reasonable budgets and timelines, Campbell Rogaliner says.

Another important factor is the lawyer's responsiveness, she says. How often does he or she communicate with clients, and what is their personal policy on response time for client phone calls and emails?

"The lawyer's general demeanor and ability to be collaborative are important considerations, regardless of the task you're hiring the lawyer to handle," Campbell Rogaliner says. "An attorney can be a zealous advocate, firm and aggressive when necessary in support of your position, but at the end of the day, he or she should also be personable, responsive to your organization's culture, and able to collaborate with you as an external member of your team, to ensure that your organization's goals and priorities dictate the way a matter is handled."

## State Laws May Apply

Be aware of any particular state statutes or regulations that require special expertise, says **Janice Merrill**, JD, shareholder with Marshall Dennehey in Orlando. For instance, Florida requires statutory prerequisites for bringing a claim for medical negligence. Other states use similar statutes.

"I can't emphasize enough how important it is to have someone who actually has experience in handling these cases. Just a generic defense attorney is not going to be enough," she says.

Merrill recalls a case transferred to her after the long-term care facility defendant first went to another attorney because they were in the same religious community. The attorney made multiple errors in handling the case before the defendant realized it needed someone more experienced in that field.

"Don't hire someone because they were recommended by a friend or family member, or because they handled a premises case for you," she says. "Look for a firm that actually tries cases. There are a lot of firms that are good at charging you money to work up cases, and then caving in settlement before trial. If you have certain cases that you're targeting for trial, you want someone with credibility in going to trial so the plaintiff knows that in negotiations."

It is important to determine the scope of what you are looking for this counsel to do, notes **Carol Michel**, JD, partner with Weinberg Wheeler Hudgins Gunn & Dial in Atlanta. Does the hospital want this attorney or firm to handle medical malpractice, general negligence, corporate negligence, or some combination of those?

Further, look for counsel that is experienced with defending particular types of healthcare organizations, Michel says. The specific issues and concerns will be different for hospitals, outpatient centers, or long-term care facilities.

"You also need to choose someone who fits your needs subjectively. You want someone you are comfortable talking to, someone who communicates in a style that works for you, and be part of a team approach," she says.


## EXECUTIVE SUMMARY

Risk managers may be involved in helping choose outside counsel for the hospital or health system. There are many factors to consider before making the right choice.

- The client and counsel should set clear expectations about fees, response times, and other issues.
- Either a large firm or a small firm could work well.
- The attorney or law firm should have adequate experience in relevant areas of healthcare law.

## Not Just Med/Mal

Remember that healthcare expertise is useful in legal matters outside of medical malpractice, says **Zachary Rothenberg**, JD, partner with Nelson Hardiman in Los Angeles. An employment issue may seem like it is the same no matter who the employer is, but that often is not the case, he says.

"You might think any employment litigator could handle it, but there are going to be opportunities along the way for an experienced healthcare lawyer to help their client," Rothenberg says. "You want someone who knows the industry, the regulations that may have some influence on the case. Those may not be apparent to you or to an employment lawyer who doesn't know your particular field."

Good healthcare counsel will have a deep enough understanding of applicable law to provide useful guidance, says **Mark R. Ustin**, JD, partner with Farrell Fritz in Albany, NY. That is more than just understanding what the law says, he explains.

"There are lots of people who can read the applicable statutes and regulations and tell you what they say, but you want someone who has their finger on the pulse of how the regulators think," Ustin says. "That narrows down the pool a lot. You will find many attorneys who have a fine understanding of what the law says but not that many who can go a step further and help you understand what means for you, and where those laws and regulations might be headed in the future." ■

### SOURCES

- Janice Merrill, JD, Shareholder, Marshall Dennehey, Orlando, FL. Phone: (407) 420-4411. Email: jlmerrill@mdwcg.com.
- Carol Michel, JD, Partner, Weinberg Wheeler Hudgins Gunn & Dial, Atlanta. Phone: (404) 832-9510. Email: cmichel@wwhgd.com.
- Wendi Campbell Rogaliner, JD, Partner, Bradley Arant Boult Cummings, Dallas. Phone: (214) 257-9841. Email: wrogaliner@bradley.com.
- Zachary Rothenberg, JD, Partner, Nelson Hardiman, Los Angeles. Phone: (310) 203-2800. Email: zrothenberg@nelsonhardiman.com.
- Mark R. Ustin, JD, Partner, Farrell Fritz, Albany, NY. Phone: (518) 313-1403. Email: mustin@farrellfritz.com.
- Edward T. Waters, JD, Managing Partner, Feldesman Tucker Leifer Fidell, Washington, DC. Phone: (202) 466-8960. Email: ewaters@feldesmantucker.com.

# Top Factors to Consider in Choosing Outside Counsel

This list of factors to consider in choosing outside counsel is offered by **Robert H. Iseman**, JD, partner with Rivkin Radler in Albany, NY.

**• Assessment of risk tolerance.** Healthcare is a high-risk business. The client should conduct an honest self-assessment of its risk tolerance and whether it is seeking a law firm that is more risk averse or willing to take reasonable risks.

**• Enterprise risk management (ERM).** Ask the firm about its view of ERM plans, the ERM process, and its experience in this area. Many firms practicing in the healthcare arena have no experience with ERM.

**• ERM experience.** The best lawyers in this area often have backgrounds in litigation, which gives them a better understanding of practical problems, not just hypothetical ones. The approach to ERM from the perspective of the client and the law firm must be in the context of the complexity of healthcare regulation and risks.

**• Directive advice.** Many lawyers advise their clients by offering available alternatives. Few lawyers tell their clients what they would do if they were in their client's shoes.

"I believe it is important to give clients what I refer to as 'directive advice' so that the client knows exactly what decision I would make if I were in the client's position. This is especially important in areas that involve a high degree of legal risk," Iseman says. "The ultimate decision about what to do rests entirely with the client, where it belongs, but the client knows where the lawyer stands. Not all clients will want this, but most will."

**• Cultural compatibility.** Lawyers have different styles of practicing. Likewise, clients have their own manner of conducting business. The culture and manner of practice of the law firm should be compatible with the culture and manner of doing business of the client. For example, to what degree does the client wish its counsel to become involved in such areas

as governance, business strategy, and other services that are not purely legal in nature? What is the client's tolerance for risk, and is it compatible with the law firm?

• **Stability.** Movement of lawyers from firm to firm in the healthcare field is not uncommon. However, such events can negatively affect clients who either must engage new counsel or follow their lawyers to a new firm. Clients should inquire about how long the healthcare attorneys have been with the firm and try to get a sense of stability, especially in the specialized healthcare practice.

• **Breadth of services.** The firm should provide "one-stop shopping" for legal services. A large healthcare delivery system faces the same legal issues as any other large business, such as labor and employment issues, personnel and benefits, vendor contracts, and capital financing.

"In addition to these general issues, healthcare systems also must confront the extremely specialized and complex regulatory overlay applicable to healthcare," Iseman says. "The law firm should possess sufficient depth and experience to handle the full range of legal issues, from the more generic to the highly specialized."

• **Responsiveness and availability.** The client should ensure it is the law firm's practice to return email messages and phone calls the same day, and that the firm has the depth of personnel to accommodate emergent situations.

• **Relationship partner.** The client should identify and be comfortable with a designated relationship partner who will be responsible to the client and to the firm for the management of the engagement.

• **Openness to nontraditional fee arrangements.** The firm should show demonstrable and genuine sensitivity to the client's budget and ability to pay professional fees. This means matching legal fees to the nature of the task undertaken by the lawyer, and the willingness to "push down" less demanding work to young associates and paralegals.

"Beyond that, the client should ask whether the hourly rates proposed by the firm are consistent with the rates being paid by other clients, or whether some clients are paying less," Iseman says. "Moreover, the firm should be open to being paid on a lump sum basis for particular engagements, lump sum retainers, and other arrangements that encourage rather than discourage the client's executives from picking up the phone and accessing the advice of counsel."

• **Added value.** The client should ask the law firm how it adds value. This includes the willingness of the firm to provide education for the client's employees in various legal areas, including risk management, and to provide similar assistance without compensation.

• **Conflicts of interest.** Clients should inquire about the other healthcare clients represented by the firm to ensure that there are no disqualifying conflicts of interest. Both business conflicts and legal conflicts should be considered carefully.

"For example, it may not be legally disqualifying for a law firm to represent one of the potential client's competitors, but such a business conflict may not be satisfactory to the client," he says. "Beware of the law firm's promise to 'wall off' those having a conflict."

• **Use of technology.** Technology is an important part of efficiency. The law firm should show that it is committed to the use of technology in the interest of efficiency and controlling the cost of legal services.

• **Other fees and expenses.** Clients should ask about whether the law firm charges for electronic legal research, intraoffice conference, clerical overtime, and other similar expenses that sometimes are billed and sometimes not billed, depending on the law firm.

• **True depth of experience.** Clients should consider whether the firm has a true depth of experience and accomplishment in all areas of the law.

"Naturally, some practice areas will be stronger than others," Iseman says. "For example, many law firms hold themselves out as having practices in such specialized areas as antitrust, tax, and others, but sometimes do not have sufficient experience and depth of knowledge in such practice areas. The lesson here is, don't rely entirely on brochures and websites." ■

## SOURCE


- Robert H. Iseman, JD, Partner, Rivkin Radler, Albany, NY. Phone: (518) 641-7055. Email: robert.iseman@rivkin.com.


## COMING IN FUTURE MONTHS

- HHS easing some requirements
- Prioritizing scant funds, resources
- New ideas in fall prevention
- When a doctor sues the hospital

HEALTHCARE RISK MANAGEMENT™



# CME/CE INSTRUCTIONS

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

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

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

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

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

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

# CME/CE QUESTIONS

1. **What does Roger D. Strode, JD, say the recent *Clovis* and *Marchand* decisions in Delaware mean for healthcare organizations?**

   a. They may face higher risks of medical malpractice liability.
   b. Their board members may be at higher risk of shareholder lawsuits and personal liability.
   c. Hospitals will be under more scrutiny for who is appointed to boards of directors.
   d. Their boards of directors may be at lower risk of shareholder lawsuits and personal liability.

2. **What does Strode say is a main message from the *Clovis* and *Marchand* decisions?**

   a. The courts are making clear that boards must actively monitor compliance.
   b. The courts are making clear that boards are not responsible for monitoring compliance.
   c. The courts are indicating that although boards should monitor compliance, they cannot be held liable for failure to do so.
   d. The courts are indicating that board efforts to monitor compliance are not material to claims of negligence or malfeasance.

3. **What does Susan L. Montminy, MPA, RN, BSN, CPHRM, CPPS, say is a key element in an adverse event response plan?**

   a. A commitment from leadership that support and guidance is available 24 hours a day.
   b. Inclusion of union representation for discussions with staff members.
   c. A promise that staff members can review and revise their comments after interviews.
   d. A unified, cohesive story from all participants in the event.

4. **What does Robert H. Iseman, JD, suggest is a potential problem when considering law firms as outside counsel?**

   a. They have no experience with enterprise risk management.
   b. They are dishonest about their experience with healthcare issues.
   c. They may be staffed mostly with junior associates and few experienced lawyers.
   d. They may have a bad track record with the outcomes of healthcare cases.

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

# Failure to Remove Sponge Results in $10.5 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*

***Elena N. Sandell**, JD*
*UCLA School of Law, 2018*

**News:** A jury awarded a woman $10.5 million after hospital staff failed to remove a sponge after surgery and failed to inform the patient of the sponge when it was discovered. According to the hospital's procedural rules, staff were required to count sponges at the beginning and end of each procedure. However, during this patient's surgery, this standard was not followed, possibly because the surgeon accidentally cut one of the patient's veins and several sponges were used to repair the damage.

The sponge eroded into the patient's intestines and remained in the patient's body for five years, causing significant injuries. Following a trial, a jury awarded the patient $10.5 million for her pain and suffering. Liability was divided among the hospital, the surgeon, and physicians who initially discovered the sponge but failed to inform the patient.

**Background:** A 54-year-old patient who suffered from diabetes entered the hospital in 2011 to undergo heart surgery. During the surgery, the operating physician accidentally cut a vein near the patient's kidney. Due to the severe blood loss, the hospital's staff used 12×12-inch surgical sponges. The procedure was completed successfully; however, the patient suffered from gastrointestinal problems shortly after the surgery.

On March 23, 2015, the patient presented to the ED complaining of severe abdominal pain, nausea, vomiting, and diarrhea. A CT scan of the patient's abdomen and pelvis revealed a metallic sponge inside her intestines. Physicians discovered one of the sponges used during the 2011 heart surgery was left inside the patient, and slowly eroded into her intestines, causing her discomfort and gastrointestinal problems. Although the radiologist who performed the CT scan informed the physicians of the presence of the metallic sponge marker, the information was not relayed to the patient, who was discharged with a prescription for anti-nausea medication. The patient's symptoms did not subside. Throughout her follow-up visits with physicians, the patient was not informed about the presence of the sponge.

NINETEEN MONTHS AFTER THE INITIAL DISCOVERY, THE SPONGE WAS FINALLY SURGICALLY REMOVED, ALTHOUGH IT HAD MIGRATED FURTHER INTO THE PATIENT'S INTESTINES.

In late November 2016, the patient was rushed to the hospital in an ambulance complaining of severe pain, vomiting, and diarrhea. Nineteen months after the initial discovery, the sponge was finally surgically removed, although it had migrated further into the patient's intestines. The patient's recovery required extended bed rest and immobility, during which she developed wounds on her feet. Such wounds, paired with her diabetes and worsened by her lack of movement, eventually developed into ulcers. Due to the severity of the injuries, physicians performed a below-the-knee amputation on her left leg. Throughout the five-year period during which the sponge remained in the patient's body, she experienced

gastrointestinal issues, including pain from the sponge partially obstructing her intestines. Furthermore, as a consequence of her recovery from the surgery, the patient developed ulcers on her feet which necessitated amputation of the patient's left leg.

The patient filed a medical malpractice lawsuit against the hospital, surgeon, and the physicians who discovered the sponge but failed to timely notify her. The patient alleged the care she received fell below the applicable standard of care, and caused her prolonged pain and suffering, including the amputation of her leg. Specifically, the patient alleged the hospital staff was negligent by not adhering to the proper procedure, which required counting sponges before and after surgery. Additionally, the patient claimed the radiologist and the physician violated the applicable standard of care by failing to inform the patient of the sponge after the first CT scan was performed in 2015, which caused the patient's injuries to significantly increase.

The defendants denied liability, and argued the amputation was inevitable due to the patient's worsening diabetes, obesity, former smoking history, and overall poor health. After a two-week trial, a jury found that all the defendants were negligent, and awarded the patient with $10.5 million. The jury apportioned 60% liability to the hospital, 15% to the physician who failed to inform the patient about the sponge, 15% to the healthcare center at which she recovered in 2016, and 10% to the initial surgeon who performed the heart surgery.

**What this means to you:** Several instances in this unfortunate matter indicate care that fell below the applicable standard. During the initial surgery, the physician's inadvertent cutting of the patient's vein caused the series of events that resulted in the patient's pain, suffering, and leg amputation. The patient's arguments were supported by strong evidence, including signed medical records that revealed at least two physicians knew about the sponge in 2015 after the first CT scan was performed, as well as written hospital policy instructing staff how to count medical tools, including sponges, at the beginning and end of each procedure.

The facts of the case left little doubt as to whether hospital staff had violated their duty of care. In addition to the ethical requirement to tell the patient about the retained sponge, there is a licensing and regulatory requirement as well. Had a sponge count been performed, the staff would have immediately discovered the discrepancy before closing, and the missing sponge could have been located and promptly removed. A portable X-ray would have facilitated prompt removal, and prevented any injury. At that time, or when the first X-ray was read when the sponge was noticed, the care provider who discovered the sponge was obligated to raise the issue and pursue it as an "adverse event" to be dealt with according to the hospital's policy and in coordination with applicable risk management and peer review procedures. The policy would require notification to the patient or patient's surrogates. The behavior of the hospital administration, operating room staff, chief of surgery, chief of staff, and medical staff caring for the patient all participated in inadequate care resulting in litigation that probably could have been avoided if the proper procedures were followed.

Unsurprisingly, the defendants could not present any compelling arguments that would justify or explain leaving a surgical sponge inside a patient's body, and subsequently failing to disclose its presence to the patient for almost two years after its initial discovery. The defendants tried to argue the loss of the patient's left leg was not a consequence of botched surgery and sponge removal procedure, but an inevitable consequence that was linked to the patient's poor health and worsening diabetes. Thus, according to the defendants, the alleged malpractice and substandard care had not caused any permanent damage in the patient since the sponge was removed in 2016.

However, the plaintiff explained that under the "eggshell plaintiff" theory, physicians and care providers take the patient "as she comes," meaning that any consequences that stem from a patient's pre-existing condition, if linked to the alleged malpractice, are considered for the damage calculations and become the responsibility of the defendants. This is a difficult situation for physicians and care providers because it may be possible to argue the patient's harm was caused by other factors — including the patient's own fault or from other serious medical conditions — but such arguments are not always successful.

Causation is a necessary element of medical malpractice cases, and a viable option for physicians and care providers to challenge as part of defending malpractice actions. In this case, the main question faced by the jury was whether the leg amputation had been caused by the patient's lack of mobility during her recovery from surgery or, as the defendants argued, was a separate issue caused solely by the patient's diabetes. As argued by the patient, although her diabetes certainly contributed to the development of the cuts and ulcers,

if she was not bedbound to recover from the sponge-removal procedure, she would have avoided developing those cuts and ulcers — or at a minimum, the injuries would not have become infected, and would have healed easier. A successful medical malpractice defense is entirely dependent on the facts and circumstances for that specific case. Physicians and care providers should work closely with counsel and experts to evaluate the particular aspects of the patient's case susceptible to challenge, including causation. ■

## REFERENCE

Decided on Dec. 30, 2019, in the Circuit Court for Jefferson County, Kentucky, Case Number 17-CI-002453.

# Appellate Court Reverses Summary Judgment Based on Expert's Disqualification

**News:** A 68-year-old patient sustained neurological damage in her right arm after a hospital's radiologic technologist failed to properly place an IV in her vein, and instead injected contrast dye directly in the patient's tissue. The patient filed a medical malpractice lawsuit against the hospital. During trial, the defendant hospital brought a motion for summary judgment, seeking an expedited adjudication based on the lack of any material issue. The trial court granted the defendant's motion.

The patient appealed the decision, which ultimately was reversed. The appellate court found the technologist was qualified to render an expert opinion on the medical causation of the patient's injuries, and that an issue of material fact existed as to whether the alleged negligent behavior was the proximate cause of the patient's injuries. The matter was sent back to the trial court.

**Background:** On June 8, 2015, a 68-year-old patient entered a hospital for a scheduled CT scan with contrast dye. The scan was to be performed to rule out a pulmonary embolism. Previously, the patient had undergone the same test without experiencing adverse effects. At the hospital, the patient warned the radiologic technologist that she had always been a "hard stick," to which the technologist replied that she had been performing the job for 25 years. After inserting the IV into the patient's right forearm, the technologist left the room and went behind the barrier to avoid radiation. At this point, a 30 mL test dose of dye was injected into the patient's arm. The injection was controlled remotely from behind the protective barrier.

As the dye entered the patient's system, she immediately started complaining of pain. The patient's pain grew in intensity and she realized that the dye was entering her tissue and not her vein, which she claimed to have shared with the technologist. The entire dose of the contrast dye was injected, and the patient was placed into the X-ray machine. As soon as the scan began, the patient began screaming in pain and asking to be taken out of the machine because the pain had become too severe and had moved from her arm to her shoulder.

According to the technologist's statement, within five or six seconds of the injection, the technologist was unable to visualize any contrast in the patient's chest. A second technologist arrived, and inserted a new IV into the patient's left arm. The dye was injected through the new IV, and the scan was repeated. During this second scan, the patient did not experience any pain. Prior to discharge, the technologist noticed a small swelling on the patient's right arm and suspected that an infiltration had occurred. She applied a dressing around the patient's arm, and warned the patient that she may experience bruising and swelling. The technologist did not notify the hospital's radiologist about the infiltration. Within a few hours of returning home, the patient's arm became so swollen that her flesh broke open and discharged fluid. After calling the hospital's imaging department and explaining what happened, the patient was instructed to alternate hot and cold compresses and go directly to the ED if her conditioned worsened. Around 10 p.m. on the evening of her discharge, the patient presented to the ED, where she was given morphine for her pain. She underwent surgery for what was diagnosed as severe IV contrast extravasation.

The patient filed a medical malpractice suit, alleging the initial IV and injection, as well as the failure to timely treat it on discovery, constituted negligence. The patient claimed that she suffers daily pain throughout her arm, diminished strength, and involuntary spasms, in addition to the substantial emotional pain and suffering. The defendant denied liability and filed a motion for summary judgment, seeking to resolve the litigation before trial based on a lack of any material issue of fact. The defendant's motion was based on the patient's expert witness, arguing that

the expert was unqualified. The trial court granted summary judgment, but an appellate court reversed that determination.

**What this means to you:** This case demonstrates the importance of expert witnesses, which not only can determine a case at trial, but even potentially before trial. Although the outcome of this case remains uncertain, and the patient has not been awarded any monetary damages, the appellate court ruling certainly is a setback for the defendant care provider, and reopens a window of opportunity for the patient to continue the allegations of malpractice.

The defendant hospital initially was successful in obtaining a successful defense judgment based on undermining the patient's expert witness. Although the ruling was reversed on appeal, not all patients are capable of appealing or pursue such appeals. Early challenges may prove invaluable for defense care providers.

The court granted the defendant's motion for summary judgment and determined the plaintiff's expert witness was not qualified to provide an opinion. In fact, while both sides recognized that a genuine issue of material fact existed as to whether the plaintiff's injuries had been caused by the dye and as to whether the technologist had failed to follow hospital policy, the defense proffered that a radiologic technologist was not sufficiently qualified to offer expert testimony, and the plaintiff had failed to present any evidence in favor of her argument.

The trial court ruled in favor of the defendant and granted the hospital's motion for summary judgment. The patient appealed the motion, arguing that a radiologic technologist was sufficiently qualified to offer expert opinion as to whether the injuries sustained by the patient could have been caused by the contrast dye. In its analysis, the appellate court discussed the applicable rules on expert witnesses. While recognizing that nonpracticing physicians could not offer expert testimony, the rule was not a "blanket rule." Specifically, regarding the medical causation issue, if the issue is not complex, a nonphysician healthcare provider may testify, provided he or she has acquired sufficient expertise through experience.

The patient's expert radiologic technologist witness provided an affidavit in which he asserted that the hospital's radiologic technologist violated hospital protocol in the administration of the contrast dye, and that it was his professional opinion that the negligence in administering the contrast dye directly and proximately caused the patient to suffer from injuries including neurological damage. When inserting an IV, the technician should have visualized blood rushing back into the IV catheter. If no blood visualized, then the catheter is not in the vein. Furthermore, if a patient complains of pain during an infusion, it should be stopped and an assessment immediately made as such levels of pain are not normal. According to the patient's expert, the failure to re-evaluate constitutes medical malpractice.

Given the appellate decision and the facts of the case, it seems the patient will be able to present a compelling argument. Specifically, the events that occurred in the imaging room indicated the hospital's radiologic technologist did not respond to the patient in a timely manner. As the test dose of the dye was injected, the patient informed the technician that she was experiencing pain. As the patient explained, it was not her first time receiving this type of scan, and she had not previously experienced any discomfort. This information alone should have been sufficient to warn the technologist that something was abnormal since the patient's reaction to the dye was substantial pain. The fact that the patient did not experience any discomfort when the second technician placed a new IV in the patient's other arm and began injecting the dye is further evidence confirming the initial inadequate care.

Another lesson from this case is the importance of listening to a patient's concerns and complaints, and taking appropriate, prompt action. In this case, the patient complained about significant pain from administration of the first IV, and such substantial pain is atypical. Patients inherently experience different pain tolerances, but some procedures objectively should not cause such levels of pain to warrant complaint beyond minor discomfort. This especially is true for patients who have experienced the procedure before and have a frame of reference. When undergoing the same procedure, but with different pain results, something may be wrong. Physicians and care providers, including hospital staff, should be aware of patient complaints and evaluate when such complaints warrant action, or when such complaints are to be expected for procedures that inherently involve a higher level of pain. Starting an IV and administering fluids through an IV objectively should not incur more than minor discomfort. Care providers should carefully evaluate patients complaining of substantial pain under unusual circumstances. The failure to do so when a reasonable physician under the same or similar circumstances would do so may constitute malpractice. ■

## REFERENCE

Decided on Oct. 29, 2019, Court of Appeals of Indiana, Case No. 19A-CT-844.

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

# Expect More High-Tech Breaches, Attorney General Audits This Year

The trend for HIPAA compliance is toward more breaches and complex breaches than seen in earlier years of efforts to follow the privacy rule, say some experts. A sharp increase in cyberattacks also may be coming this year. Most HIPAA breaches in the past were of a rather low-tech nature, even if they involved lost computers and data files. Laptops were stolen, jump drives were lost, and paper documents were mishandled. But that is changing now, partly because the digital revolution has completely changed how healthcare organizations handle data, says **Steven Marco**, CISA, ITIL, HPSA, president and founder of HIPAA One, a consulting group in Lindon, UT.

"It used to be that the breaches were not very frequent. When they happened, they often involved the theft of electronic media. That type of physical data loss represented your highest likelihood of having to report a breach," Marco says. "Server incidents were almost unheard of. We've seen a drastic change with a trend toward each incident involving more individuals, rather than many incidents involving a small number. Each cyber incident now typically involves tens of thousands of individuals. That trend is not changing any time soon."

The nature of attacks on covered entities is changing at the same time, says **Bobby Seegmiller**, senior vice president and founding partner of HIPAA One. Healthcare organizations have become much savvier about how to protect their data from outside threats, but they still struggle with internal security, he says.

"Some of these hospitals are like Fort Knox with all the security they have to keep someone from coming in either physically or through a cyberattack — but their own employees are leaving the back door wide open," Seegmiller says. "The hospital puts up all this security and it is undermined by the employee who opens an email and responds to a phishing attack."

Employee training is critical, but that is not enough, Seegmiller stresses. It is important to test employees periodically with a real-world scenario such as sending a fake email that includes all the hallmarks of a phishing attempt and see who takes the bait, he says. "We're finding that about one in three will click on the link," he says.

Marco predicts that cyber security attacks will increase by 50% in 2020. "There is an industry for cyber criminals that did not exist years ago. There is a market on the dark web for financial information and private information that is driving these criminals to work harder and find new ways to access this product they need to sell," Marco observes. "We will see more use of ransomware also, because organizations are paying the ransom, and the criminals know that every hospital needs to make payroll. If [criminals] see that it works, they will keep trying to get ransomware into your systems."

Marco also notes there have been ransomware attacks in which the healthcare organization refused to pay the ransom and did not report a breach, but still accessed data from backups. In those cases, the danger may not be over if the hackers could access protected data.

"I would anticipate that these hackers will get frustrated and eventually start releasing PHI [protected health information] from those organizations that did not pay," Marco says. "Any organization in that position should be prepared for that possibility and have a plan in place for responding. It is possible that any patient whose PHI was released could complain to Health and Human Services, and it's now a reportable breach."

New compliance requirements also are possible in 2020. This will put added stress on covered entities to bolster their HIPAA protections at the same time they need to do more to protect themselves against cyberattacks, Marco explains.

"There's a big push for privacy right now, and there is a good chance HIPAA will be amended to align with the public sentiment in favor of patients having more control over their health information," he predicts.

Seegmiller notes the likelihood of undergoing an Office for Civil Rights audit also has increased in recent years. The rate of

audits several years ago was so low that covered entities believed they would never be audited and grew lax in some areas of compliance, particularly the risk assessment requirement, he explains.

"We're seeing a new trend with state attorneys general, who were deputized in the HITECH Act in 2009 to conduct these audits, getting more interested in HIPAA audits. It may be because they saw that the feds were collecting all these penalties from their audits, even though they were infrequent, and they saw a chance to get in on that," Seegmiller observes. "It's a revenue source. We're seeing more attorney general audits that we didn't see in the past."

Marco notes there are simple steps for improving HIPAA security that often are overlooked. For example, the commonly used Microsoft Office 365 software includes privacy and security options that can be effective in reducing vulnerability to cyberattacks, but covered entities do not activate them, he says. Using two-factor authentication also can be highly effective in deterring fraudulent logins, Marco adds. This method usually requires sending a simple code to the authorized user's mobile phone to verify the person's identity before completing the login process.

"Multifactor authentication with a code sent by text message wards off 99.999% of attacks trying to compromise user accounts," Marco says. "That's a huge measure of safety that requires little investment or effort." ■

# HIPAA Settlements Hold Lessons on Right of Access, Breach Reporting

The Office for Civil Rights (OCR) recently announced two HIPAA settlements that offer lessons for covered entities regarding right of access and failure to notify after a breach.

In early 2019, OCR announced it would take steps to enforce the rights of patients to receive copies of their medical records timely and at a reasonable cost. This led to the introduction of the HIPAA Right of Access Initiative.

In September 2019, OCR issued a penalty to Bayfront Health St. Petersburg, FL, a fine of $85,000.[1] This was the first enforcement action and settlement under this new initiative. In December, OCR settled a second case, this time with Korunda Medical in Florida, which agreed to take corrective actions and pay an $85,000 fine.[2]

In a press announcement about the Korunda settlement, OCR explained the Right of Access Initiative was the agency's promise to "vigorously enforce the rights of patients to get access to their medical records promptly, without being overcharged, and in the readily producible format of their choice."[2]

The settlement addressed a patient complaint alleging Korunda failed to forward a patient's medical records in electronic format to a third party despite numerous requests. "Not only did Korunda fail to timely provide the records to the third party, but Korunda also failed to provide them in the requested electronic format, and charged more than the reasonably cost-based fees allowed under HIPAA," OCR said.[2] "OCR provided Korunda with technical assistance on how to correct these matters and closed the complaint. Despite OCR's assistance, Korunda continued to fail to provide the requested records, resulting in another complaint to OCR."

**Ryan Meehan**, healthcare senior manager of Schellman & Company, a global independent security and privacy compliance assessor based in Tampa, FL, explains that the regulation from which these cases and fines are emerging can be traced to the HIPAA Privacy Rule requirements under §164.524, which concerns an individual's access to protected health information.

Specifically, he says, these cases seem to revolve around the requirement that "the covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement."[3]

"While the Bayfront case focused on significant delays — nine months when the standard requires it to be submitted in the proper format within 30 days — the Korunda case is notable in that the format in which the files were eventually provided to the individual was not appropriate and the cost to the individual for access to their ePHI was not reasonable," Meehan says. "The OCR came in to provide technical assistance after the initial complaint was received, but the case had to be reopened as Korunda was still noncompliant. This is the first case in which the format and cost are being considered and factored into a fine from the OCR."

In looking at the fines Korunda received, Meehan says it is worthwhile for risk managers and compliance officers to revisit the HIPAA requirements on which the fine is based. He cites these provisions:

- Privacy Rule § 164.524(b)(2)(i): "…the covered entity must act on a request for access no later than 30 days after receipt of the request as follows";
- Privacy Rule § 164.524(c)(2)(i): "The covered entity must provide the

individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual."

• Privacy Rule § 164.524(c)(2): "If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee."[3]

While there are defined exceptions noted within the standard, Meehan says "it is clear that the OCR is taking seriously the effort for individuals to access their ePHI. In the case of Korunda, this is now extending beyond just the timeliness of those individuals receiving their ePHI; it also extends to include the format and cost associated with the request."

Meehan stresses the importance of reviewing how individuals might request information and if the organizations can meet those requests appropriately. "Decide whether there is confidence that the records can be provided timely, that the records are kept in an appropriate manner that has been defined and known by the individual, and that there is a justifiable and reasonable cost associated with providing those requests to the individual," Meehan explains.

The key takeaway from the Korunda settlement is the necessity of respecting basic compliance obligations, says **Matthew R. Fisher**, JD, partner with Mirick O'Connell in Worcester, MA. When considering the individual right to access, the right has been around as long as the privacy rule, he notes. Further, the parameters around access are clear, he says. Thus, delaying a response or giving an individual a runaround is not something that should occur.

"OCR had been making a number of public comments about focusing on the right of access. Finally getting two settlements in that regard should not have been overly surprising," Fisher offers. "The message being sent is that if organizations continue not honoring the right of access, then enforcement will follow."

Fisher notes the relatively small dollar amount of the fines, wondering "whether a sufficient message of deterrence has been made."

OCR also may be sending a message with the settlement amounts in both right to access cases, says **Matt Frederiksen-England**, CHC, CHPR, CHRC, faculty member at Walden University in Minneapolis. He notes Bayfront is a level II trauma tertiary care, with about 480 beds and more than 550 physicians, while Korunda is a much smaller provider, seeing about 2,000 patients per year. "OCR has now applied the same fines to both a large institution and a smaller provider-based office," he says. "OCR is making a statement showing they will hold all accountable to the HIPAA Privacy Rule requirements regardless of size."

The Korunda settlement signals OCR is taking a much stronger approach to making sure patients can access their information, says **William P. Dillon**, JD, shareholder with Gunster in Tallahassee, FL.

"OCR wants it to be clear that patients have a right to get access to their records, and in an appropriate format," Dillon says. "You don't have to go out and buy special software, but if it is feasible to give patients the data in the format they want, you have to do it because OCR is not going to tolerate a failure to give patients access to their data." ■

## REFERENCES


1. HHS.gov. OCR settles first case in HIPAA Right of Access Initiative, Sept. 9, 2019. Available at: http://bit.ly/2GuUEsj.
2. HHS.gov. OCR settles second case in HIPAA Right of Access Initiative, Dec. 12, 2019. Available at: http://bit.ly/2uImjmJ.
3. HHS.gov. Individuals' right under HIPAA to access their health information 45 CFR § 164.524. Available at: http://bit.ly/2RzGD2X.


# Wrong Person Receives Bill, OCR Secures $2.175 Million Fine

Sentara Hospitals in Virginia and North Carolina agreed to take corrective actions and pay $2.175 million to settle potential HIPAA violations stemming from a complaint alleging the organization sent a bill to an individual containing another patient's PHI.[1] OCR determined Sentara mailed 577 patients' PHI to wrong addresses. Sentara reported the incident as a breach affecting only eight people because they concluded (incorrectly) that unless the disclosure included patient diagnosis, treatment information, or other medical information, no reportable breach of PHI had occurred. "Sentara persisted in its refusal to properly report the breach even after being explicitly advised of their duty to do so by OCR," the office reports. OCR also determined Sentara failed to put a business associate agreement in place with another company.[1]

**Matthew R. Fisher**, JD, partner with Mirick O'Connell in Worcester, MA, says the easy lesson is not to fight with

OCR over interpretation of the regulations implementing HIPAA. Some portions of the regulations may be subject to reasonably different interpretations. However, if OCR says it believes a bigger breach than reported occurred, pushing back is destined to fail.

The common thread that runs through breach-related settlements is the requirement for companies to develop policies and procedures to comply with applicable notification regulations, says **Eric B. Stern**, JD, partner with Kaufman Dolowich & Voluck in Woodbury, NY. In fact, he says, most of the "Corrective Action Obligations" section of the "Corrective Action Plan" relates to forming and distributing of such policies and procedures.

As new privacy laws and regulations are put forth on both the state and federal levels, Stern says every covered entity should work with competent counsel to develop policies and procedures for breach preparedness, avoidance, and response that is compliant with applicable laws and regulations; conduct a bi-annual audit of the policies and procedures to ensure compliance; and follow those policies and procedures to prevent a breach and in response to one. Despite healthcare providers having to comply with HIPAA since 1996, they still continue to violate the law by failing to properly report breaches and by failing to put business associate agreements (BAA) in place, says **Sara H. Jodka**, JD, an attorney with Dickinson Wright in Columbus, OH. "These issues are HIPAA-compliance 101, yet healthcare providers are still messing these requirements up. It would be different if we were dealing with new technology issues, such as ransomware attacks or a new type of code-corrupted ERM databases, but this is not that," Jodka says. "This is failing to neglect simple, routine HIPAA compliance requirements."

Healthcare providers still have to sweat the small stuff. "Firewalls and state-of-the-art technology are critical for HIPAA compliance, but those things are just as important as proper reporting and having proper BAAs in place," she says.

**Marissa G. Weitzner**, JD, senior counsel in the Houston office of Clark Hill, noted there were three seven-figure fines levied in 2019 related to HIPAA violations. This is a sign OCR will continue its robust HIPAA enforcement.

"Sentara's self-reporting was incorrect, and its insistence on an inappropriate definition of what constitutes PHI increased its liability," she observes. "Had Sentara appropriately entered into a BAA with its parent entity, or appropriately self-reported the breach, it is unlikely it would have incurred liability for the business associate matter."

**Matt Frederiksen-England**, CHC, CHPR, CHRC, faculty member at Walden University in Minneapolis, says there are several action items these settlements might prompt for compliance:

• Review organizational policies to ensure they detail the patient's right to access medical records within 30 days of the request and the patient's right to request their medical records in a specific format, either paper or electronic;

• When releasing information, verify employees are following a practice that demonstrates compliance with the individual's right to access requirements;

• Ensure breach notification policies are up to date.

Because the HIPAA Privacy Rule allows a covered entity to perform a risk assessment, it is imperative professionals develop a tool to evaluate a potential breach before assuming an event is nonreportable. According to OCR, this tool should include the following factors:

• The nature and extent of the PHI involved, including any patient identifiers or likelihood of reidentification;

• The unauthorized person who used the PHI or to whom the disclosure was made;

• Whether the PHI was viewed or acquired;

• The extent to which risk to the PHI was mitigated;

• Ensure a policy exists regarding BAAs, and a process is in place to ensure contract and capital purchases are reviewed to ensure appropriate BAAs are in place. ■

## REFERENCE

1. HHS.gov. OCR secures $2.175 million HIPAA settlement after hospitals failed to properly notify HHS of a breach of unsecured protected health information, Nov. 27, 2019. Available at: http://bit.ly/2U1LeML.