HEALTHCARE RISK MANAGEMENT™

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

INSIDE

RELIAS
Formerly AHC Media

APRIL 2018 Vol. 40, No. 4; p. 37-48

Lawsuit Claims EHR Dangerous to Patients, Could Affect Hospitals

An electronic health record (EHR) vendor is facing a class-action lawsuit claiming that faults in the product's software threaten patient safety, and hospitals using the EHR could become entangled in the litigation. The case illustrates how healthcare organizations can face liability for defects in their EHRs.

In 2017, eClinicalWorks in Westborough, MA, agreed to a $155 million settlement to resolve a False Claims Act suit that claimed it falsified meaningful use certification and gave customers kickbacks to publicly promote its products. Now, it is being sued in a class-action complaint led by the estate of Stjepan Tot. The complaint filed in the U.S. District Court in the Southern District of New York asks for $999 million in monetary damages for breach of fiduciary duty and gross negligence. *(The complaint is online at: http://bit.ly/2Hle9Sr.)*

> MORE THAN 850,000 HEALTHCARE PROVIDERS USE ECLINICALWORKS SOFTWARE, AND MILLIONS OF OTHER PATIENT RECORDS HAVE BEEN COMPROMISED, THE LAWSUIT CLAIMS.

Before Stjepan Tot died of cancer, the complaint claims "he was unable to determine reliably when his first symptoms of cancer appeared [as] his medical records failed to accurately display his medical history on progress notes."

More than 850,000 healthcare providers use eClinicalWorks software, and millions of other patient records have been compromised, the lawsuit claims. The complaint also alleges that

Financial Disclosure: Author **Greg Freeman**, Editor **Jill Drachenberg**, Editor **Jesse Saffron**, Editorial Group Manager **Terrey L. Hatcher** 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
AHC Media, LLC, a Relias Learning company
111 Corning Road, Suite 250
Cary, NC 27518

Periodicals Postage Paid at Cary, NC, and at additional mailing offices
GST Registration Number: R128870672

POSTMASTER: Send address changes to: *Healthcare Risk Management*
Relias Learning
111 Corning Road, Suite 250
Cary, NC 27518

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, $519. Add $19.99 for shipping & handling. Online only, single user: 1 year with free CE nursing contact hours, $469. Outside USA, add $30 per year, total prepaid in USA funds.

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

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

Relias Learning is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians. Relias Learning designates this enduring material for a maximum of 1.5 *AMA PRA Category 1 Credits™*. Physicians should claim only credit commensurate with the extent of their participation in an activity.

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

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

AUTHOR: Greg Freeman
EDITOR: Jill Drachenberg
EDITOR: Jesse Saffron
EDITORIAL GROUP MANAGER: Terrey L. Hatcher
SENIOR ACCREDITATIONS OFFICER: Lee Landenberger

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

eClinicalWorks software did not meet meaningful use and certification requirements laid out by the Office of the National Coordinator for Health Information Technology (ONC), as the company claimed.

The complaint alleges numerous problems with the software, including failure to reliably record diagnostic imaging orders, insufficient audit logs, issues with data portability, and noncompliance with certification criteria.

State Law Guides Case

The eClinicalWorks case raises several important issues for healthcare risk managers, says **John C. Ivins Jr.**, JD, partner with the Hirschler Fleischer law firm in Richmond, VA. Among them are the potential exposure of a hospital or physician where the EHR system fails to accurately reflect medical information critical to the treatment of a patient, and the risk of a medical malpractice case arising out of faulty EHR systems.

Questions of liability, possible legal theories that can be advanced against a healthcare facility, system or practitioner, and the defenses that can be asserted in response all are going to be a function of state law, Ivins says. However, in general, many of these issues arise out of the vendor contract that typically is heavily negotiated and ultimately entered into between the EHR provider and the healthcare entity seeking to acquire the EHR system.

"Generally, the healthcare entity who acquires an EHR system is ultimately responsible for the system, including ensuring that all its healthcare personnel are properly trained and understand how to use the system," Ivins says. "Moreover, the 'learned intermediary' doctrine generally states that a manufacturer who provides a properly functioning EHR system has fulfilled its legal duty of care once it has provided all necessary information to the healthcare professional — the learned intermediary — who, in turn, interacts directly with the patient."

Knowing that, the vendor will seek to negotiate terms based on these concepts which relieve the vendor from as much liability as possible, he explains. The hospital, healthcare system, physician practice, or other healthcare provider must negotiate a contract that addresses as many of these issues as possible, and provides indemnification from the vendor for matters such as privacy and HIPAA breach-related damages and third-party claims for injury, Ivins says.

As a general rule, where the EHR system is systematically faulty, the odds are in the hospital's favor, Ivins says. He notes that in the 2017 FCA settlement, the Justice

EXECUTIVE SUMMARY

The vendor of an electronic health record faces a lawsuit alleging software faults hurt a patient. Hospitals could become embroiled in such litigation.

- Contract negotiations are key to minimizing potential liability.
- Proper training on use of the EHR also reduces the risk.
- Hospitals could sue the EHR vendor for providing a faulty product.

Department did not pursue the physician practices that received "meaningful use" payments based on their false attestations because of their inability to know the attestations were false under those circumstances.

"On the other hand, a suit filed by a physician practice in December against eClinicalWorks alleged that, under the same scenario, it had to forfeit certain meaningful use payments already collected," Ivins explains. "The practice said it was further damaged by having efforts to collect meaningful use payments thwarted by a Medicaid official who advised that because the practice used the same EHR system that was the subject of the FCA settlement, implementation of that system could not serve as a basis for such payments."

Hospital Can Be Involved

It is possible that a hospital can be sued or drawn into litigation based on a defect that lies solely with the EHR vendor, Ivins says. However, the key to considering any liability claim arising out of an EHR system issue is determining the cause of any alleged harm giving rise to such a claim, he says. *(See the story on page 41 for scenarios in which hospital liability is possible.)*

The best defense against such liability is to take the time and effort to thoroughly vet and select the EHR vendor and system best suited for the hospital and its needs, Ivins says. Next, with the involvement of experienced healthcare counsel, a hospital must seek to negotiate the most favorable EHR vendor contract possible.

"Hospitals will want to establish a contract-specific performance criterion against which the performance of the EHR system can be measured and address the various liability and indemnification issues discussed above," Ivins says.

There are many other contract and vendor issues that also should be addressed, and Ivins suggests referring to the key issues provided by several ONC publications, including "EHR Contracts Untangled: Selecting Wisely, Negotiating Terms, and Understanding the Fine Print" and the "Health IT Playbook." *(Those resources are available online at: http://bit.ly/2dWxmwz and: http://bit.ly/2h0vFBH.)*

Train Users Well

Once an EHR system is developed and ready for implementation, the hospital must take steps to ensure that all users are well-trained and that the implementation and transition processes do not negatively affect patient care, Ivins says. Hospitals must ensure that all systems are maintained and updated regularly, and that all users understand the systems and any updates or changes, he says.

There are a number of legal issues triggered when EHR software is inaccurate and, depending on the technology involved, they can come from many different places, says **Sara H. Jodka**, JD, an attorney with the law firm of Dickinson Wright in Columbus, OH.

Some issues come from mistakes and information gaps, such as voice-recognition software that drops words, typographical errors that lead to medication or prescription errors, misinterpretation of drop-down menus or other display functionality, reliance on old/outdated records, discrepancies in what appears electronically vs. what is printed, and errors inserted because of patient status issues.

Another issue is triggered when EHR technology is not compliant or miscommunicates regarding its compliance status, Jodka says. Any EHR must meet certain compliance standards, particularly to take advantage of the Medicare and Medicaid EHR Incentive Programs that provide financial incentives for the meaningful use of certified EHR technology.

The ONC enforces the standards and certification criteria and the final rule specifies the necessary technological capabilities EHR technology must include to be certified by an ONC-Authorized Testing and Certification Body. Additionally, it sets forth how eligible healthcare providers will need to use the EHR technology to meet these standards, Jodka explains.

When the EHR company fails to meet those standards or otherwise threatens patient safety, there is potential for patient-based lawsuits including claims for negligence (which, in some states, could include gross negligence) and breach of fiduciary duty.

"The EHR software company could also face lawsuits from their clients, which would be the hospitals, clinics, and other providers that license their software for claims including fraud, breach of contract, and promissory estoppel," Jodka says. "These types of claims would certainly be likely in cases where there were also allegations that users relied on the EHR tech company's statements that the software did and would satisfy

the certification criteria of the meaningful use program."

Hospital Blamed First

If a patient is improperly diagnosed or treated, the hospital or physician usually are the first ones blamed for the error, whatever the cause, Jodka says. Hospitals using a faulty EHR can expect to be involved, at least initially, in any litigation in which the software is later determined to be primarily responsible for the error, she says.

"The difficult issues for patients and hospitals is determining where the error occurred. This leaves hospitals as the first stop in the named defendant list in a lawsuit. Typically, the patient will not know the issue was the result of an EHR software issue, but will think it is a doctor medical malpractice issue," she says. "In most cases, the EHR software issue will not shake out until later, leaving the patient and the hospital engaging in even more litigation to get the EHR included in the suit."

In such a scenario, the hospital is likely to cross-sue the new EHR provider co-defendant for breach of contract, fraud, and whatever else may fit the circumstances, and potentially seek indemnification for the costs of its defense and any losses based on the terms of the contract language between the hospital and the EHR provider, Jodka says. In many cases, it will not be until depositions when it is determined what exactly happened and what was the exact cause of the misdiagnosis or mistreatment, she says.

"The simple fact is that there is and will continue to be a complex interplay between technology and medical practice, which has a human component that is necessarily prone to individual judgment, interpretation, and error," she says. "Technology training, installation, and other issues can also sometimes drive the issue."

So far, there have not been many suits against hospitals or medical professionals that have triggered these types of issues, Jodka says, but the rise of technology and EHR database breaches likely will spur more such litigation.

> "EHR VENDOR CONTRACTS CANNOT AND SHOULD NOT BE RUBBER-STAMPED, AS THEY FAVOR THE EHR VENDOR, LEAVING THE HOSPITAL WITH LITTLE LEGAL RECOURSE IN A BREACH SCENARIO."

Whether a hospital can be held liable for any resulting harm depends on the nature of the claim, Jodka says. If the injury is truly the fault of the EHR, the vendor likely will be responsible without the hospital incurring direct liability, Jodka says. But that might not be the case if the contract was poorly vetted and the language allows the vendor to shift some or all responsibility to the product user.

"EHR vendor contracts cannot and should not be rubber-stamped, as they favor the EHR vendor, leaving the hospital with little legal recourse in a breach scenario. Competent healthcare counsel should be consulted early on in the negotiation stage to ensure fairness, legal compliance, and accountability," Jodka advises.

"Also, opt for short-term contracts so new contract negotiations can occur and can address any issues that might have arisen during that last contract term," she adds. "A vendor that knows it's up for review tends to provide better service to close that next contract to avoid losing to the competition."

Keep EHRs Clean

Healthcare organizations also must ensure they are properly recording software issues and reporting them to the vendor. It also is important that the hospital properly train employees on the use of the EHR so the vendor can't blame any problems on human error.

"The hospital can take on the human factor by providing all employees proper and detailed training on EHR software to try to avoid the human/technology conundrum," Jodka says. "To the extent healthcare professionals are properly using the software, ensuring notes are clear and correct, typographical errors fixed, if there comes a time during litigation when finger-pointing between the hospital and the EHR vendor occurs, this could help the fault stick with the vendor rather than the hospital."

Jodka also recommends remaining vigilant for software issues regarding the EHR you're using. Watch the news and industry sources for problems other hospitals may be having with EHRs so

you identify issues to avoid or proactively address in your own organization.

It is possible for a hospital to be found liable in a case alleging faulty EHR software, says **Romaine Marshall**, JD, partner at the law firm of Holland & Hart in Salt Lake City. In the eClinicalWorks litigation, the primary legal question is whether the vendor misrepresented the functionality of its EHR software in a manner that caused failures leading to the death of the patient, he says.

The plaintiff is alleging, among other things, that the company's software failed in spite of promises that it would reliably record diagnostic images, maintain accurate treatment logs, meet certain portability requirements, and satisfy certification criteria enabling healthcare providers to qualify for government incentive payments.

"A hospital is responsible to provide reasonable care to a patient, and from the patient's view, their relationship is directly with the hospital, not the vendor providing the EHR software," Marshall says. "Thus, the potential liability for a hospital for an EHR product that is faulty is high if the functionality of the product requires intervention by a hospital, if there has been harm to a patient caused not only by faulty software but also by the improper use and application of that software."

Due Diligence Is Crucial

A hospital should use all available options and tools to protect itself before engaging an EHR software

Hospital Liability Possible with EHR-related Claims

While it may be hard to imagine the physician or hospital being held liable under the circumstances alleged in the eClinicalWorks litigation, it is only a short step to scenarios in which liability is quite possible.

John C. Ivins Jr., JD, partner with the Hirschler Fleischer law firm in Richmond, VA, offers these scenarios — all based on submitted claims — in which hospital liability may be possible:

• A child presents to his physician with a fever, rash, and flushness. The child has recently visited a country where tuberculosis (TB) was prevalent. The initial office note incorrectly indicates that the patient has not been exposed to TB, and the child is initially treated with fluids and antibiotics.

When the child returns on subsequent occasions due to his condition worsening, the copy-and-paste feature is used to copy the initial note indicating the patient was not exposed to TB. All these events lead to injuries to the child.

In this scenario, liability may hinge on whether the cause of harm was the person who initially incorrectly noted that the child had not been exposed to TB, or the EHR system that permitted the information to be repeatedly copied and pasted.

• A doctor prescribes an antibiotic for a patient indicating a certain amount of milligrams for the medication. But as this information is entered into the EHR system, the order created through the system is, instead, based upon the amount of milligrams of medication per kilogram of the patient's weight, resulting in the patient receiving many more pills than needed.

In this case, is the cause of this error the person who entered the information, or the EHR system?

• A patient presents to the ED for an injury arising from having stabbed herself with a garden fork. In addressing the patient's tetanus shot status, the intake nurse selects the dropdown option "unknown/last five years." Thereafter, the treating physician interprets this as not needing a shot, when it turns out the patient had never been immunized.

Was the cause of this error the person who entered the information, or the choices and format provided by the EHR system?

• An anesthesiologist is using the EHR but does not have information available that tells him the patient is not a candidate for the anesthesia ultimately selected, which results in harm to the patient. Is the cause of the harm the physician, or the structure of the EHR system?

"While the determination of the cause and ultimate legal impact in each scenario would be further affected by additional facts, the state's laws, and, perhaps, the terms of applicable contracts, each reveals the challenges present in considering issues of potential liability arising from the use of EHR systems," Ivins says. ■

vendor, says **Rich Spilde**, JD, partner at the law firm of Holland & Hart in Boulder, CO.

Due to the inherent risks associated with software platforms — computer systems and their networks — careful diligence is required before diving into contract discussions, Spilde says. The diligence process should include both internal diligence, where a hospital conducts its own risk assessment, reviews its own operations to determine its challenges and the type of solution to address them, and then evaluates the marketplace to determine what is most likely to meet their needs.

"Two of the biggest impacts on this process are costs and time. Everyone wants the best solution they can get for the least amount of money," Spilde says. "But the danger with these objectives is when a potential vendor offers a deal to move things along faster and the due diligence effort is minimized. The effort expended as part of the vendor selection process should be tied to the risk the contract and the solution exposes a hospital to, not merely the dollar value of the deal."

Don't Overlook Implementation

The part of the process that is most often overlooked is implementation, Spilde says. This is where details matter. It is critical to reach agreement on and to document the implementation process, each party's tasks and responsibilities, relevant milestones, and perhaps most important, testing of the solution, Spilde says.

"While the initial presentation of software has been impressive, can the same be said about the migration process for the software to the hospital's computer systems and networks? Did the hospital work through and confirm that all key record information is accurately transferred and displayed?" Spilde says. "Does the solution show the hospital the information they need?"

As for the contract itself, the risk allocation provisions, such as representations, warranties, indemnification, and liability limitation provisions demand close scrutiny, he says. Carefully address compliance functions, audits (both for compliance and information security), performance standards (measuring key metrics such as solution availability, response to problems, but also accuracy) and the effect of changeover. Finally, consider what happens if the agreement expires or is terminated.

> "THE EFFORT EXPENDED AS PART OF THE VENDOR SELECTION PROCESS SHOULD BE TIED TO THE RISK THE CONTRACT AND THE SOLUTION EXPOSES A HOSPITAL TO, NOT MERELY THE DOLLAR VALUE OF THE DEAL."

Marshall and Spilde agree that a hospital may be held liable for any resulting patient harm. A patient who is injured or harmed as a result of a problem relating to EHR software may assert a negligence claim against the hospital in the same way they can against a physician.

In the case of EHR software, an injured party might assert that the hospital failed to use reasonable care in its selection of EHR software based on a product's known problems or limitations. An injured party may also assert that a hospital failed to properly maintain its facilities and train staff, failed to properly oversee the EHR software vendor, overly relied on the EHR software instead of sound professional medical judgment, or failed to maintain accurate records in the software, whether due to input errors by the hospital or due to problems in the software itself.

"The question then becomes whether a hospital actually will be held liable," Marshall says. "If a hospital conducts reasonable due diligence about the EHR software, reasonably relies on representations about the EHR software by a vendor, and has no basis to doubt these representations, then the potential liability for a hospital when an EHR product is faulty is lower." ■

SOURCES

- **Sara H. Jodka**, JD, Dickinson Wright, Columbus, OH. Phone: (614) 744-2943. Email: sjodka@dicksonwright.com.
- **John C. Ivins Jr.**, JD, Partner, Hirschler Fleischer, Richmond, VA. Phone: (804) 771-9587. Email: jivins@hf-law.com.
- **Romaine Marshall**, JD, Partner, Holland & Hart, Salt Lake City. Phone: (801) 799-5922. Email: rcmarshall@hollandhart.com.
- **Rich Spilde**, JD, Partner, Holland & Hart, Boulder, CO. Phone: (303) 473-4808. Email: rdspilde@hollandhart.com.

EHRs Can Work Against You in Court

Electronic health records (EHRs) are a godsend for physicians and hospitals when they know they are in the right and only need a way to prove it. But healthcare providers also are finding that EHRs can sink the defense when it provides unexpected or contradictory evidence.

One issue that risk managers have noticed recently is that EHRs record not only when an entry was made in the patient chart — which everyone is aware of and wouldn't try to fake — but also where the entry was made. For instance, the EHR may reveal that the clinician was not at the bedside when the entry was made, as claimed, but at another workstation.

EHRs can hurt the defense in a number of ways, says **David Richman**, JD, partner with the law firm of Rivkin Radler in Uniondale, NY. He has seen a number of cases in which a doctor's defense was compromised by an EHR, but it is more often the result of the software package being used in the doctor's office than any wrongdoing on the doctor's part.

Richman notes that several years ago, when EHRs were becoming more prevalent in physicians' offices, the software would lock the notes once they were created. Consequently, if a doctor wanted to make a change, he or she would have to create a new note. More times than not, the second note was not an exact recreation of the earlier note, but instead added or omitted information.

"Because the software did not allow the user to state that this was an amendment to an earlier note, it appeared as though two or more notes were created for the same visit. The discrepancies provided plaintiff's counsel with ample material for cross-examination," Richman says. "In one early case, the doctor wound up creating seven notes for the same visit, none of which matched up, making the case very difficult to defend."

Another software-related pitfall that Richman and his colleagues continue to see with some regularity involves notes carrying forward from one office visit to the next.

"This is likely a function of user error or misuse, and perhaps driven by insurance company requirements. Too many times, the note is simply carried forward without any alteration despite the fact that the patient was seen and examined, and new findings were made," he says. "The failure to document those new findings makes it appear that nothing took place at the visit despite clear indications to the contrary, such as lab work or radiology reports."

An EHR can be a blessing or a curse when defending a medical negligence case, says **Dennis Harms**, JD, shareholder with the law firm of Sandberg Phoenix in St. Louis. Information contained in the EHR, but not included in the legal medical record, adds depth to key evidence in the case.

However, the clinician's access to the EHR makes him or her responsible for knowing all the information included there.

"The EHR potentially demonstrates that provider's knowledge of any data contained in the EHR at that time. Thus, if the timing of an intervention, such as a medication order, is an issue in the case, then plaintiff's counsel can preclude, to some extent, a defense based on a lack of information necessary to require that intervention," Harms says.

On the other hand, defense counsel can use the same timing data to demonstrate that the provider acted immediately when presented with critical data. Such immediacy can support a defense that even the best of care was insufficient to prevent an adverse event, he says.

"The worst-case scenario occurs when the EHR demonstrates that the provider altered the record to make events appear more favorable in the event of litigation," Harms says. "In these cases, defense counsel are faced with spoliation and punitive damage claims in addition to those already present in complex medical negligence litigation." ■

EXECUTIVE SUMMARY

Electronic health records (EHRs) can be used against you in court. The record may provide evidence contrary to what the defendant claims.

- EHRs can record where, not just when, an entry was made.
- Locked notes can create confusion with added information.
- Timing data can both help and hurt a case.

SOURCES

- **Dennis Harms**, JD, Shareholder, Sandberg Phoenix, St. Louis. Phone: (314) 446-4252. Email: dharms@sandbergphoenix.com.
- **David Richman**, JD, Partner, Rivkin Radler, Uniondale, NY. Phone: (516) 357-3120. Email: david.richman@rivkin.com.

Tips on Career Advancement Include Finance, Enterprise Risk Management

Patient safety should be a top priority for risk managers hoping to advance their careers, and financial management may be another way to set yourself apart from the crowd.

There is a marked trend toward the importance of patient safety, says **Arnold Mackles**, MD, MBA, LHRM, president of Innovative Healthcare Compliance Group in Beach Gardens, FL.

"Risk managers have traditionally been concerned with the reporting and investigation of adverse events, claim management, and overseeing the organization's liability insurance policies. Risk managers are now becoming more involved with creating an environment that provides safe, quality patient care," Mackles says. "As a matter of fact, many hospitals now recruit for the position of director of patient safety and risk management."

Given this trend, it would be wise for risk managers and others aspiring to work in this arena to consider membership in professional organizations that specialize in patient safety, such as the American Society of Professionals in Patient Safety (ASPPS), Mackles says. He strongly recommends obtaining a certification as a Certified Professional in Patient Safety (CPPS).

Mackles notes the recent merger of two influential organizations in the patient safety field, the National Patient Safety Foundation (NPSF) and the Institute for Healthcare Improvement (IHI), which he says is further evidence of the growing focus on patient safety.

Another trend that is receiving widespread acceptance is the notion of a "culture of safety" in healthcare organizations, Mackles says.

"The future will see risk managers playing important roles in creating environments that are open and transparent, where the reporting of medical errors and unsafe practices is rewarded rather than punished," Mackles says. "Other hallmarks of a culture of safety include constant striving for safer care, cooperation and communication across all specialties and hierarchies, buy-in and support by leadership, and an obligation of healthcare administrators to resolve safety issues."

Risk managers wanting more expertise in data science should look to gaining a foundation in several areas, says **Craig Johnson**, founder and chief science officer at Decision Point Healthcare Solutions, a data and technology company based in Boston. He recommends the following four areas:

- **Clinical or business subject matter expertise:** a working knowledge of the stakeholders, business processes, data collected and used by those processes, and how information is shared within and across those processes.
- **Feature and data engineering:** ability to identify and design key clinical/business data features, characterize the relationships between those features, and how to best represent those features in data.
- **Programming:** ability to program in a functional programming language like python, analytic tools like R, and database languages like SQL.
- **Technical methods:** understanding of the conceptual methods and application of those methods in solving clinical/business problems. Technically oriented pathways will dive deeper in to algorithm programming and development.

"With these underlying experiences/skill sets, data scientists can focus on building deeper skills focused on a business or technology track," Johnson says. "Entry to the technical data science track typically follows undergraduate and graduate study in data analytics, data science, physics, mathematics, or operations research. Subject matter expertise and feature engineering skills can be learned during the first few years on the job."

Entry to the business data science track typically follows several years of on-the-job experience as a clinical or business data analyst, then going back to school for a degree in data analysis or data science, Johnson says. Exceptions to this

EXECUTIVE SUMMARY

Patient safety continues to be a primary focus in risk management. Those interested in advancing their careers also might look to data science and finance.

- Enterprise risk management should be part of your career plan.
- The popularity of captive insurance companies puts a premium on finance knowledge.
- Data science is increasingly central to understanding risk.

include undergraduate/graduate programs like healthcare and nursing informatics, and business degrees with concentrations in data analytics. However, these programs do not typically provide sufficient depth in the underlying technical side of data science, he says.

Finance is another route to consider, suggests **M. Michael Zuckerman**, JD, MBA, ACI, professor in the department of risk, insurance, and healthcare management at Temple University Fox School of Business and Management in Philadelphia.

Clinical risk managers who want to broaden their risk management capabilities should consider pursuing the Associate in Captive Insurance professional designation from the International Center for Captive Insurance Education (ICCIE).

"Most healthcare systems employ captive insurance companies, and this designation does provide courses in alternative risk financing, reinsurance, and healthcare captive overview," Zuckerman says. "This is by far the most rigorous alternative risk financing and captive insurance educational material available. It is taught online by industry professionals."

Enterprise risk management (ERM) also should be considered for career advancement, suggests **Jay Lechtman**, senior director of healthcare market strategy and development for Riskonnect, a healthcare ERM software vendor.

"When I ask patient safety and risk managers if their organizations are getting into enterprise risk management, they too often wave vaguely toward compliance and the executive suite and say 'they're doing it … over there,'" Lechtman says. "Traditional risk managers have a significant career opportunity to elevate and broaden their current roles by getting involved in ERM, and a significant career risk if they don't."

> "IT SEEMS LIKE A NATURAL EVOLUTION AND A LOGICAL EXPANSION IN ROLE FOR TRADITIONAL RISK MANAGERS WHO CAN BE FLEXIBLE, STRATEGIC, AND COMFORTABLE WITH EXECUTIVE LEADERSHIP AND BOARDS OF DIRECTORS."

Lechtman recalls talking recently to a health system compliance vice president who is driving her organization's ERM initiative. When he asked her about the patient safety and patient grievance teams, she admitted that she didn't really know what they did.

"These and other traditional risk managers will be committing career suicide if they aren't connecting what they do every day with clinical, financial, operational, regulatory, and strategic risks and the value they bring to the organization at the highest levels," he says. "It seems strange to me that enterprise risk management in healthcare is very often not being led by — sometimes not even with the participation of — traditional healthcare risk managers."

Don't think of ERM as a separate, siloed function, Lechtman advises. Instead, think of it as managing risk across the enterprise.

"It seems like a natural evolution and a logical expansion in role for traditional risk managers who can be flexible, strategic, and comfortable with executive leadership and boards of directors," he says. ■

SOURCES

- **Craig Johnson**, Chief Science Officer, Decision Point Healthcare Solutions, Boston. Phone: (617) 459-4550.
- **Jay Lechtman**, Senior Director of Healthcare Market Strategy and Development, Riskonnect, Kennesaw, GA. Phone: (770) 790-4700.
- **Arnold Mackles**, MD, MBA, LHRM, President, Innovative Healthcare Compliance Group, Beach Gardens, FL. Phone: (561) 762-1906. Email: amackles@comcast.net.
- **M. Michael Zuckerman**, JD, MBA, ACI, Department of Risk, Insurance and Healthcare Management, Temple University Fox School of Business and Management, Philadelphia. Telephone: (215) 204-8144. Email: zuckerm@temple.edu.

$3.5 Million Settlement Highlights Risk Analysis

A health system's recent settlement with the government shows how providers still are dropping the ball on compliance issues that everyone should understand by now.

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced recently that Fresenius Medical Care North America (FMCNA) agreed to pay $3.5 million for HIPAA violations.

The violations at the heart of the case show how healthcare organizations still are not up to speed on the need for risk analysis, says **Roy Wyman**, JD, partner with the law firm of Nelson Mullins Riley & Scarborough in Nashville, TN. He recalls recent government research on HIPAA compliance that illustrated the shortcoming.

"A large proportion of the covered entities surveyed flunked it entirely, with a lot of them having done absolutely nothing in risk analysis," he says. "You combine that with this settlement with Fresenius and you see that what really nailed them was not the disclosures, but the fact they had not done a risk assessment to figure out where the risks were."

People get overwhelmed and don't know where to start with a risk assessment, Wyman says.

"They'll grab the low-hanging fruit with things like putting the privacy practices in place, but what they don't realize is that there is this basic security requirement," Wyman says. "Once OCR gets in the door, it's the first thing they're going to look for. It's almost always overlooked — not just in small practices, but in hospitals and large entities. They're missing this entirely."

Assessment May Be Pricey

To be sure, conducting a proper risk assessment is no small endeavor. Wyman worked in the past with a large healthcare organization to conduct a full risk assessment and saw how much money and work it requires.

"For a big organization, you were talking about paying six figures for a firm to come in and do a full assessment, and then at the end of it they haven't fixed anything. They've just told you what you need to do," Wyman says. "You still aren't compliant because you haven't incorporated it into your risk management program."

Companies with billions of dollars in revenue every year can afford to do that, Wyman says, but the typical physician practice or hospital relies on far less sophisticated measures for HIPAA compliance.

Covered entities can conduct a proper risk analysis internally, Wyman says, but most will require the guidance of an attorney specializing in HIPAA compliance.

Wyman notes that OCR's enforcement has changed focus recently, no longer looking for breaches and looking more for failures to comply with essential components like the risk analysis.

"These days, they aren't actually looking for harm," Wyman says. "We're seeing people hit with very large fines where no information was disclosed. Now with failure to have a risk assessment, it's usually tag-along where there's some small disclosure but they say that's no big deal — but the failure to have a risk assessment is a big deal."

CAP Also Required

In addition to the settlement, FMCNA also will adopt a comprehensive corrective action plan, OCR announced. FMCNA provides products and services for more than 170,00 patients with chronic kidney failure. On Jan. 21, 2013, FMCNA filed five separate breach reports for separate incidents occurring between Feb. 23, 2012, and July 18, 2012, implicating the electronic protected health information (ePHI) of five separate FMCNA-owned covered entities, according to the OCR report.

"OCR's investigation revealed FMCNA covered entities failed to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of its ePHI," the report says. "The FMCNA covered entities impermissibly

EXECUTIVE SUMMARY

A large health system will pay $3.5 million to settle allegations it violated HIPAA. The case illustrates the need for better risk analysis.

- The health system failed to conduct a risk analysis.
- The Office for Civil Rights is focusing less on disclosure and more on risk analysis.
- Risk assessments can be expensive, but can be performed internally.

disclosed the ePHI of patients by providing unauthorized access for a purpose not permitted by the Privacy Rule."

Various locations of FMCNA failed to implement policies and procedures to address security incidents; failed to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility; failed to implement policies and procedures to safeguard their facilities and equipment from unauthorized access, tampering, and theft when it was reasonable and appropriate to do so under the circumstances; and failed to implement a mechanism to encrypt and decrypt ePHI when it was reasonable and appropriate to do so under the circumstances.

"The number of breaches, involving a variety of locations and vulnerabilities, highlights why there is no substitute for an enterprisewide risk analysis for a covered entity," OCR Director **Roger Severino** said in a statement announcing the settlement. "Covered entities must take a thorough look at their internal policies and procedures to ensure they are protecting their patients' health information in accordance with the law."

In addition to a $3.5 million monetary settlement, a corrective action plan requires the FMCNA covered entities to complete a risk analysis and risk management plan, revise policies and procedures on device and media controls as well as facility access controls, develop an encryption report, and educate its workforce on policies and procedures.

The resolution agreement and corrective action plan can be found on the Office for Civil Rights website at: http://bit.ly/2nwTvXi. ■

SOURCE

- Roy Wyman, Partner, Nelson Mullins, Nashville, TN. Phone: (615) 664-5362. Email: roy.wyman@nelsonmullins.com.

Hospital and Cardiology Group to Pay $20.75 Million

A Pennsylvania hospital and cardiology group have agreed to pay the government $20.75 million to settle a False Claims Act lawsuit alleging that they knowingly submitted claims to the Medicare and Medicaid programs that violated the Anti-Kickback Statute and the Physician Self-Referral Law, the Department of Justice (DOJ) announced recently.

The settlement involves University of Pittsburgh Medical Center Hamot, a hospital based in Erie, PA, and now affiliated with Medicor Associates, a regional physician cardiology practice.

The Anti-Kickback Statute prohibits offering, paying, soliciting, or receiving remuneration to induce referrals of items or services covered by Medicare, Medicaid, and other federally funded programs. The Physician Self-Referral Law, commonly known as the Stark Law, prohibits a hospital from billing Medicare for certain services referred by physicians with whom the hospital has an improper compensation arrangement.

The DOJ announced that the settlement resolves allegations brought in a whistleblower action filed under the False Claims Act alleging that, from 1999 to 2010, "Hamot paid Medicor up to $2 million per year under 12 physician and administrative services arrangements which were created to secure Medicor patient referrals. Hamot allegedly had no legitimate need for the services contracted for, and in some instances the services either were duplicative or were not performed."

Acting Assistant Attorney General **Chad A. Readler**, JD, head of the DOJ's Civil Division, said. "Financial arrangements that improperly compensate physicians for referrals encourage physicians to make decisions based on financial gain rather than patient needs. The Department of Justice is committed to preventing illegal financial relationships that undermine the integrity of our public health programs."

DOJ reports that the lawsuit was filed by a physician who worked for Medicor from 2001 to 2005, under the *qui tam*, or whistleblower, provisions of the False Claims Act, which permits private parties to sue on behalf of the government when they believe that defendants submitted false claims for government funds and to share in any recovery.

The U.S. District Court for the Western District of Pennsylvania held that two of Hamot's arrangements with Medicor violated the Stark Law and the case was set for trial when the United States helped to facilitate the settlement. The whistleblower physician will receive $6,017,500.

The lawsuit is available online at: http://bit.ly/2p9D1VI. ■

HEALTHCARE RISK MANAGEMENT™

CME/CE INSTRUCTIONS

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

1. Read and study the activity, using the provided references for further research.
2. Log on to AHCMedia.com to take a post-test, then select "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.

CME/CE QUESTIONS

1. **What is the base claim made in the lawsuit alleging the eClinicalWorks electronic health record (EHR) was faulty?**

   a. The patient was unable to determine reliably when his first symptoms of cancer appeared because the EHR failed to accurately display his medical history on progress notes.
   b. The EHR incorrectly identified the patient and merged his records with those of another patient.
   c. The EHR was unavailable to clinicians at a critical point in his care.
   d. The patient was misled by inaccurate information in the EHR and made a wrong decision about treatment.

2. **What does John C. Ivins Jr., JD, say regarding the potential liability of healthcare providers for a vendor's faulty EHR?**

   a. State laws vary, but the individual contract will have significant influence.
   b. State laws will not apply and only the contract will determine liability.
   c. State laws determine liability and the contract has no influence.
   d. State laws generally do not address the issue of liability for a vendor's failure.

3. **Why does David Richman, JD, say locked notes can be detrimental to the defense in healthcare litigation?**

   a. The notes are unavailable to clinicians who need the information to continue care.
   b. Amendments may appear as though two or more notes were created for the same visit.
   c. Locking the note can give the impression that the clinician was hasty in documentation.
   d. A locked note conveys that the clinician was hiding something.

4. **According to Roy Wyman, JD, how has the Office for Civil Rights changed its compliance focus regarding HIPAA?**

   a. It no longer focuses on small healthcare providers.
   b. It no longer focuses on violations older than two years.
   c. It is no longer looking for disclosures, focusing more on compliance issues like risk analysis.
   d. It is no longer focusing on compliance issues and is only looking for disclosures of protected information.

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

Physician on Probation Places Patient in Unnecessary Coma, Yielding $9 Million Verdict

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

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

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

News: A man presented to a local hospital for treatment of gallstones. The treating physician induced a coma, but left the patient untreated for a month due to a misdiagnosis. Notably, the physician had been placed on probation, and was on probation at the time of treatment for similarly negligent care of a similarly situated patient. After a month, the hospital sought a second opinion from another physician who promptly operated on the patient without complication.

Despite the correct diagnosis and prompt operation by the second physician, the patient suffered substantial injuries. The patient filed suit against the hospital and the first physician. A jury awarded the patient $43 million, which was reduced pursuant to a high-low arrangement between the parties.

Background: In April 2014, a 61-year-old man presented to a hospital for the treatment of stomach pain and vomiting. Upon analyzing the patient's condition, a physician erroneously diagnosed the patient with an anatomical abnormality he said would make surgery to remove bile duct stones impossible. As a result, the physician placed the patient in a medically induced coma for more than a month. During that time, the patient was effectively abandoned by the physician and hospital personnel.

The hospital eventually sought a second opinion on the patient's condition. A different physician rejected the initial diagnosis, revived the patient, and performed surgery without complication. Despite the successful surgery, the patient suffered serious and incapacitating injuries as a result of the extended coma and required a liver transplant. His injuries ultimately left him unable to continue work as a chemicals company vice president.

THE PHYSICIAN PLACED THE PATIENT IN A MEDICALLY INDUCED COMA. DURING THAT TIME, THE PATIENT WAS EFFECTIVELY ABANDONED BY THE PHYSICIAN AND HOSPITAL PERSONNEL.

Following these events, the patient filed suit against the initial physician, the hospital, and others, alleging that the hospital was negligent in allowing the initial physician to treat the patient.

Of particular importance to this negligence claim is that the physician was previously placed on probation by the state medical board. In June 2013, the state medical board found glaring deficiencies in the physician's treatment of a patient similarly situated to the patient in this case. In the analogous case, the board determined that the physician failed to adequately document the patient's records, inaccurately diagnosed the patient, and performed medically unnecessary procedures. For example, the board found that the physician inaccurately described the location of a patient's ulcer and falsely claimed that he had performed multiple biopsies to test for cancer.

The case proceeded to trial, and the parties entered into

a high-low agreement whereby the patient was guaranteed no less than $4 million and limited to $9 million. At trial, evidence demonstrated that despite hospital policy requiring automatic suspension of physicians on probation, the hospital permitted this physician to continue practicing. According to the lawsuit, hospital administrators prohibited a medical executive committee review of the physician's hospital standing.

After the five-day trial, the jury returned a verdict in favor of the patient for approximately $43 million. The verdict comprised approximately $18.5 million for past and future pain and suffering, lost earnings and medical care, and $25 million in punitive damages. The jury found the hospital 90% liable and the physician 10% liable. Because of the high-low agreement, the verdict is immune to the state's statutory cap on noneconomic damages, and the recovery will be reduced to $9 million.

What this means to you: One of the many mistakes made by the medical professionals and hospital in this case was the failure to adequately monitor patients. Patients require consistent — and sometimes constant — monitoring and care, and this is particularly true for comatose patients. To leave a patient unattended for a month is to beg for a costly lawsuit.

A potential method for preventing the abandonment of a patient is to develop and implement a workflow of reviews based on date landmarks with respect to all patients. This workflow must require actionable plans to be developed where feasible. Regulations require daily progress notes by an attending physician be documented in the patient's medical record. Appropriate date-based landmarks should be based on a patient's condition, and perhaps based on the department in which the patient is being treated. For example, patients in the ICU and ER would have much tighter time frames than non-urgent patients undergoing recovery after routine operations. Regardless of the method by which the workflows are generated, they must be created based on the applicable standard of care.

Another mechanism for preventing stagnation of treatment is early second opinions. This is especially valuable in situations such as the present case, where an initial physician's suggested treatment appears patently unreasonable. Second opinions should be written into patient care workflows, with the additional safeguard that they are triggered where no actionable plan can be created.

If medical support staff feel disempowered to seek a second opinion, hospitals may consider implementing an anonymous secondary review procedure. This can involve a second physician reviewing the medical record without alerting the primary care physician — essentially an audit of the patient's file. Many hospitals use nurse case managers to review appropriateness of care on a daily basis, who can review the medical plan of care as documented by the physician and communicate unusual or unnecessary practices to a utilization review committee. That committee's leader can then intervene to correct or amend the plan of care.

This case also raises concerns about physician probation and other corrective procedures. The hospital's policy to automatically suspend physicians on probation is an excellent measure to reduce medical malpractice, but only if it is actually implemented. Permitting a physician on probation to practice medicine raises increased risk for negligence claims. Even if the physician adheres to the standard of care, disgruntled patients may use the probationary status as leverage in litigation that is otherwise in the hospital's favor. A more advisable course of action is to suspend physicians from practicing medicine during the probationary period.

A less severe alternative is to proctor physicians on probation. This allows the physician to be observed and mentored by a more senior and experienced physician who can evaluate the probationer's progress while assuring the safety of his or her patients. Proctoring enables a hospital's peer review committee to make a well-informed decision to either reinstate the physician with full privileges or proceed toward permanent removal of the physician. Hospitals should support their physicians and provide them with resources to return to good standing with medical boards, if the hospital considers the physician capable of returning to standard employment with the hospital. Establishing such a clear path avoids situations where a physician is suspended indefinitely, as that offers finality to neither the physician nor the hospital.

Finally, this case presents an issue that plagues hospitals and other businesses: ensuring that procedures and initiatives are not only implemented, but are actually followed. This can be a difficult task, but it must be prioritized for the procedures to have any meaningful impact. If a hospital finds it necessary to develop a policy, failure to see it practiced is nothing more than a waste of time and resources. Furthermore, it can be argued as evidence of negligence in malpractice litigation. Taking this case as an example, the hospital's bylaws mandated the suspension of physicians who are

placed on probation. The hospital knew such physicians should not practice medicine, yet the hospital failed to follow its own procedures and instead let the probationer continue to practice. Jury members may be persuaded that a hospital failing to follow its own procedures is evidence of negligence, thus eliminating any potential advantage from having a beneficial policy in place in the first instance. Thus, it is critical for hospitals to ensure that medical professionals and staff are aware of the policies and adhere to them. ■

REFERENCE

Decided on Jan. 20, 2018, in the 241st District Court in Smith County, Texas; case number 16-0853-C.

Negligent Presurgery Procedure Results in Fatal Pulmonary Arrest, $5.5 Million Verdict

News: In August 2012, a middle-aged man suffered a knee injury. He sought treatment and was released from a hospital with a splint. He sought surgery for his injury and met with another physician for presurgery consultation. During the consultation, a Doppler test was performed that returned a normal result. The patient was cleared for surgery, and returned to the hospital for the procedure.

The patient complained to the surgeon of continued pain, swelling, and a heating sensation in his leg. No additional Doppler test was administered. The patient was anesthetized for the surgery, and a blood clot detached from his leg and traveled to his lung, causing a pulmonary embolism. The patient was declared brain dead and ultimately died. The patient's estate successfully argued in litigation that the presurgery procedures were negligent and that he should have received a second Doppler test. The subsequent lawsuit yielded a $5.5 million verdict.

Background: A 44-year-old electrical engineer suffered a knee injury on Aug. 7, 2012. He initially sought treatment at an emergency room, and was released with a splint on his leg. The patient presented to a different hospital on Aug. 9, and the treating physician referred the patient to a surgeon who also worked at the hospital. Surgery was scheduled for Aug. 16.

After the visit, the patient called the physician complaining that his splinted left knee, calf, and leg felt hot. The physician sent approval for the patient to undergo Doppler imaging of his left leg at a hospital. The Doppler was performed on Aug. 10 and the results were sent to the physician. The imaging was negative for any abnormalities in the leg.

On the morning of Aug. 13, the patient presented to the second hospital and was cleared for the Aug. 16 surgery to repair ruptured ligaments in his knee. The patient was anesthetized, and soon after suffered a pulmonary embolism when a deep vein thrombosis in his left leg detached and traveled to his lung. He suffered pulmonary arrest, coded, and was declared brain dead within hours of arriving for surgery.

The presurgical clearance was performed by a nurse practitioner, and the patient had a consultation with the surgeon who was scheduled to perform the surgery. The patient allegedly reported that he had continuing pain, swelling, and heat sensation in his left leg. Relying on the Doppler performed a few days earlier, the surgeon told the patient that the symptoms were related to the knee trauma he suffered. No additional Doppler imaging was ordered or performed despite the patient's continued symptoms.

The patient was declared brain dead on Aug. 16, 2012, and died Aug. 19, 2012. He remained unconscious through the final four days of his life and was survived by his wife and two daughters.

The patient's estate filed suit against the physicians, nurse practitioner, the hospital, and its faculty practice. The estate claimed that the various defendants were negligent in failing to order a second Doppler image of the patient's left leg. The estate alleged this second test was necessary because the patient's symptoms — continued pain, swelling, and perceived heat — were consistent with a deep vein thrombosis. Moreover, the estate argued that the first Doppler image was taken too close in proximity to the injury to reveal the deep vein thrombosis, as they typically take time to grow and develop after injury.

The defense argued that the patient's signs and symptoms did not change after the Doppler on Aug. 10 and, therefore, there was no reason to order a second Doppler prior to performing surgery. The defense further argued that the nurse

practitioner was not allowed to order a Doppler, knew the surgeon would see the patient during the same visit, and could rely on the surgeon to order the necessary presurgical tests.

Before trial, the physicians and nurse practitioner were dismissed from the case. A trial ultimately proceeded against the second hospital and its faculty practice. After an 11-day trial, a verdict was delivered in favor of the estate against the hospital faculty practice, awarding more than $5.5 million for personal injury and wrongful death.

What this means to you: This case illustrates the need for communication in the healthcare industry. In this case, a breakdown in communication occurred interhospital, intrahospital, and between patient and medical professional. Preparing a satisfactory medical record does a great deal for solving the inter- and intrahospital issues. It is important for medical records to be clear enough that any medical professional who picks up a patient's file can determine exactly what steps have been taken and potentially what the next steps should be. If that practice is followed, the practice of medicine will be significantly more efficient when patients are transferred between hospitals and departments within hospitals.

Another lesson from this case is the importance of adequate and thorough presurgery procedures. Many presurgery procedures include interviews with the surgeon and other physicians knowledgeable in the various systems of the body likely to be affected by the surgery, such as a cardiologist for patients with a history of heart complications or a hematologist for patients with symptoms of blood clots or a family history of blood clots. Presurgery examinations also typically involve various tests. Some tests should be required for all patients scheduled for particular surgeries, such as complete blood count tests, X-rays, and ECGs. Specific factors may trigger the need for certain tests, such as the patient's age, particularly difficult surgeries, and other health risks. Finally, many presurgery interviews are conducted at least a month in advance of operation. As a result, a thorough presurgery procedure should include a follow-up closer to the operation. Regardless of the tests and physician consultations used, hospitals should make an effort to establish hospitalwide minimums.

The ultimately fatal condition in this case, deep vein thrombosis, has several symptoms and risk factors that healthcare professionals should be familiar with to avoid substantial injury to patients and potential malpractice claims. While it is possible for deep vein thrombosis to not be accompanied by symptoms, swelling in one or both legs, pain or tenderness in the legs, warm skin on the legs, skin discoloration, visible veins, and tired legs all are potential symptoms that should prompt medical professionals to check for deep vein thrombosis. By analyzing both risk factors and symptoms, medical professionals can more readily diagnose and treat a deep vein thrombosis and prevent pulmonary embolisms.

Radiological misreads are common in healthcare for multiple reasons. Preliminary reads often are performed by technicians who are licensed to take measurements of the various organs and/or anomalies seen in the films or on the screens and document them for a radiologist to review. Unfortunately, it is common for a technician to include a diagnostic term, and a busy radiologist may accept this and proceed to use it in the final report without independent validation. This poses a danger to hospitals and radiologists, as acceptance without review may constitute a failure to provide the applicable standard of care.

Another common reason for a misread is the subjectivity often expressed in a radiologist's interpretation of a result. A common example is differentiation between a tumor, fatty cyst, or other type of lesion. In cases where a patient's symptoms warrant a study that is initially interpreted as negative, if the same symptoms persist or worsen, a re-read of the original study should be made. If the review continues as negative, a prudent physician often orders a repeat of the study. By documenting all of this in the patient's record, the provider reduces the risk of future involvement in any subsequent litigation.

Many states have enacted laws that limit the scope of work that can be performed by nurse practitioners — for example, many states limit nurse practitioners' ability to prescribe medicine. Many large states (such as California, Texas, and Florida) require physician oversight to prescribe, diagnose, and treat patients. However, other states have enacted laws that afford nurse practitioners full prescriptive authority, permitting them to prescribe, diagnose, and treat patients without the supervision of a physician. It is vital that hospitals are familiar with their state's laws, and make them clear to their nurse practitioners as well as physicians. Violations of such laws, including permitting unauthorized nurse practitioners to prescribe medicine, open the door to penalties and malpractice liability. ■

REFERENCE

Decided on Jan. 23, 2018 in Cook County Circuit Court, Illinois; case No. 2014-L-006816.