HEALTHCARE RISK MANAGEMENT™

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

INSIDE

AHC Media
A RELIAS LEARNING COMPANY

JULY 2017 Vol. 39, No. 7; p. 73-84

Cyberattack Shows Threat to Patient Safety, Liability Risks

The threat to patient safety and the potential for resulting liability from a cyberattack was illustrated in the recent WannaCry attack that crippled the United Kingdom's National Health Service (NHS) and affected thousands of organizations around the world. American risk managers should count themselves lucky their hospitals and health systems weren't hit as hard, but the effect could be much worse next time.

The malware in the global cyberattack, also known as WanaCrypt0r 2.0 WannaCry and WCry, infected computers in 150 countries, entering IT systems via an email attachment and encrypting data files, including patient records. The hackers demanded ransom to unencrypt the files. The malware caused many hospitals and clinics in the NHS to close their doors for fear that patient safety would be threatened without access to electronic medical records (EMRs) and other computer files.

Healthcare providers should have been prepared for this because it is nothing new, says **Marc S. Voses**, JD, partner with the law firm of Kaufman Dolowich Voluck in New York City, and co-chair of its data privacy and technology services practice. It is just the scale of the event that is unique, he says.

> MANY PROVIDERS, INCLUDING THE NHS, TURNED OUT TO BE THE SOFTEST TARGET BECAUSE TIGHT BUDGETS RESULTED IN A FAILURE TO FUND CYBERSECURITY.

Healthcare providers were not a special target for the hackers in this attack, Voses says, but many providers, including the NHS, turned out to be the softest target because tight budgets resulted in a failure to fund cybersecurity.

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

HEALTHCARE RISK MANAGEMENT™

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

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

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

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

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

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

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

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

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

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

AUTHOR: Greg Freeman
EDITOR: Jill Drachenberg
EDITOR: Jonathan Springston
AHC MEDIA EDITORIAL GROUP MANAGER: Terrey L. Hatcher
SENIOR ACCREDITATIONS OFFICER: Lee Landenberger

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

"The NHS didn't have the money to upgrade from the Windows XP operating system, which was at end of life in 2014, which means there were no more patches available from Microsoft," Voses says. "Even if you could afford to update your software, you still might not be able to because you have other dependent software that is vital to running your business and will run only on the outdated, unpatchable operating system."

The WannaCry ransomware attack hit U.K. healthcare organizations especially hard because many internet-connected medical devices are running older versions of the Windows operating system, says **Moshe Ben-Simon**, co-founder and vice president of services at TrapX, a company in San Mateo, CA, providing cybersecurity defense. In most cases, the healthcare providers know the devices are out of date but still face hurdles in plugging the security holes.

"Due to compliance regulations, including HIPAA, healthcare network administrators cannot easily update internet-connected medical devices with the newest operating systems and patches. These devices are sealed to protect the equipment from failure in the event a software update inadvertently affects the operation of the device," Ben-Simon says. "While this ultimately protects patients from potential harm from a malfunctioning device, it has the potential to leave the network open to attackers who are finding new ways to exploit old vulnerabilities, such as the recent WannaCry attack. If these devices aren't updated by the manufacturers immediately, they will continue to be susceptible to these types of attacks."

Risk Management Must Anticipate Attacks

Any potential electronic disturbance that disrupts healthcare services must be addressed in a healthcare provider's risk management protocol, Voses says. Prompt access to backup files and systems is necessary to minimize the damage caused by these types of catastrophes, he says.

"This is going to happen again. Having protocols in place to either ignore the threat and shift to backup systems or a plan to promptly pay the ransom to acquire the encryption key is of paramount importance," Voses says. "Yet again, luck favors the prepared."

Voses notes that cyberthreats to patient safety are not new, though the risk appears to be growing. On Feb. 17, 2016, he points out, Hollywood Presbyterian Medical

EXECUTIVE SUMMARY

The recent worldwide cyberattack highlighted the vulnerability of healthcare computer systems. The United Kingdom's National Health Service was virtually crippled by the attack.

- Experts expect more such cyberattacks on healthcare organizations.
- Legacy computer systems and internet-connected medical devices offer openings to hackers.
- The U.S. government has proposed sweeping improvements in healthcare to safeguard against future attacks.

Center paid a ransom in bitcoins equivalent to about $17,000 to hackers who infiltrated and disabled its computer network. On March 28, 2016, MedStar Health, a nonprofit healthcare organization headquartered in Maryland, also was attacked by ransomware.

Although MedStar denied there was any significant effect because they quickly shut down their computer system, some employees stated that the virus still disabled access to patient records, Voses says. The hackers demanded 45 bitcoins (the equivalent of about $19,000) in exchange for the decryption key.

In addition to requiring payment, a ransomware attack could result in liability if the computer system breach is severe and involves key operating data, Voses says. For example, if a hospital lost access to its computer systems, patients' lives may be at risk.

Voses says that the risk of an organization falling victim to a ransomware incident is increasing due to the shotgun approach taken by criminals to find victims.

Backup Processes Vital

To better protect hospital networks that are using internet-connected medical devices, Ben-Simon recommends reviewing and beefing up backup processes. It is essential to run an offsite backup daily, he says, and more important is a robust, tested disaster recovery process that ensures core IT systems can be brought back up in a few hours.

"Most hospitals have backup in place to support compliance, of course, but really cannot restore key applications and recover operations fast enough in the face of a ransomware attack. When an environment faces a true disaster, even a well-planned disaster recovery strategy will typically take days until full operations are restored," he says. "Do the work to make sure this takes only a few hours."

In addition to keeping software systems updated and other technological barriers, there are methods to counterattack malware if it does get into the computer system. Ben-Simon's company uses technology that employs deception to stop an attacker in the network before the attack can take a substantial foothold, tying up the ransomware encryption process with false data on decoy network shares. Deception tools are designed to fool attackers and their ransomware exploits, keeping them from your real devices and real data, Ben-Simon says.

"Once they start trying to encrypt these fake file systems, they will be identified, shut down, and the hospital can return to normal operations," he explains.

Ransomware attacks on healthcare organizations are likely to increase, says **Stacy Leidwinger**, vice president of products at RES, a company in Radnor, PA, that provides digital workspace software addressing the risk of ransomware. The fact that some NHS hospitals and clinics had to suspend all non-urgent activity is a testament to how much they rely on their data to operate, she says.

"It's becoming more common an occurrence to see ransomware attacks against healthcare organizations. After all, they are a prime target for attackers due to the nature of the data they hold," she says. "The real problem is that it's not just a monetary loss when it comes to medical facilities. It's life and death."

The WannaCry attack is clear evidence that many healthcare organizations still need to invest in an integrated approach to security, Leidwinger says. The most important defenses are education, vigilance, and proven technology such as context-aware access controls, comprehensive blacklisting and whitelisting, read-only access, automated access termination, and adequate back-up, she says.

Feds Recommend Security Fixes

Immediately after the WannaCry attack, the federal Health Care Industry Cybersecurity Task Force released a draft "Report on Improving Cybersecurity in the Health Care Industry," which addresses the identified risks and offers a substantial number of proposed recommendations and action items for Congress, the Department of Health and Human Services (HHS) and other government agencies, and private industry.

The authors concluded the recent attack should be a wake-up call for the healthcare industry.

"With the exception of IT security personnel, many providers and other healthcare workers often assume that the IT network and the devices they support function efficiently and that their level of cybersecurity vulnerability is low. Recent high-profile incidents, such as ransomware attacks and large-scale privacy breaches, have shown this vulnerability assumption to be false and provided an opportunity to increase education and awareness about the benefits of cybersecurity in the healthcare community," according to the report. "Moreover, recent ransomware incidents have

also highlighted how patient care at healthcare delivery organizations can be interrupted due to a system compromise. Members of the health ecosystem reported that prior to these breaches, many security professionals had difficulty demonstrating the importance of cyberprotections to organizational leadership, including how risk mitigation can save money and protect against reputational damage in the long-term. Making the decision to prioritize cybersecurity within the healthcare industry requires culture shifts and increased communication to and from leadership, as well as changes in the way providers perform their duties in the clinical environment."

(The full report is available online at: http://bit.ly/2ssHkfB. See the story below for sample advice from the report.)

The task force's recommendation for a unified response to cybersecurity issues for the healthcare industry is of vital importance, says **Lee G. Petro**, JD, an attorney with the law firm of Drinker Biddle in Washington, DC.

The report's recommendations extend throughout both government and private industry, and highlight the urgent need for the identification and empowerment of an individual within HHS to coordinate the varied effort, Petro notes.

"The proposal reflected a comprehensive approach to considering the need for cybersecurity protections across the widely diversified healthcare industry. The proposal's reliance on existing National Institute of Standards and Technology [NIST] frameworks reflects the importance of NIST's work and the need for the completion of its efforts to update to the Cybersecurity Framework Version 1.1," Petro says.

Several of the report's action items will affect seemingly nonrelated federal laws and statutes, necessitating the close coordination between the executive branch and Congress, Petro notes. The financial effect on agency budgets will be significant, and will need to be taken into consideration during budget negotiations, he says.

"The recommendations that will impact small- and medium-sized healthcare providers will also be significant, possibly impacting their financial health in the short-to-medium-term future," he says. ■

SOURCES

- **Stacy Leidwinger**, Vice President of Products, RES, Radnor, PA. Telephone: 1 (800) 893-7810.
- **Lee G. Petro**, JD, Drinker Biddle, Washington, DC. Telephone: (202) 230-5857. Email: lee.petro@dbr.com.
- **Moshe Ben-Simon**, Co-Founder and Vice President of Services, TrapX, San Mateo, CA. Telephone: (855) 249-4453.
- **Marc S. Voses**, JD, Partner, Kaufman Dolowich Voluck, New York City. Telephone: (212) 485-9600. Email: mvoses@kdvlaw.com.

Task Force Advises Review of Healthcare Cybersecurity

After the WannaCry cyberattack hit healthcare providers and other organizations worldwide, the federal Health Care Industry Cybersecurity Task Force released a report that offers recommendations for action to be taken by the healthcare industry, Congress, HHS, and other groups.

The following are some of the recommendations:

• Recommendation 1.2: Establish a consistent, consensus-based healthcare-specific Cybersecurity Framework.

In other critical infrastructure sectors, a framework helped establish a consensus-based standard for improving the conversation around cybersecurity, the report notes. "Although NIST has developed a generic framework, healthcare (like other sectors) has many unique aspects such as its diverse resource capabilities, legacy systems that will persist for years, and the burden of the need to have low barriers for sharing of data that is essential for collaborative patient-oriented care," according to the report. "The framework should build upon the minimum standard of security required by the NIST Cybersecurity Framework and the HIPAA Security Rule to promote a single lexicon for healthcare sector as well as standards, guidelines, and best practices. The complex environment requires certain basic standards that all stakeholders must meet and guidelines that allow flexibility for select issues. Without this framework, any of the countless constituents may pose a risk to the healthcare ecosystem."

• Recommendation 1.5: Explore potential effects to the Stark Law, the Anti-Kickback Statute, and other fraud and abuse laws to allow large healthcare organizations to

share cybersecurity resources and information with their partners.

The task force heard many concerns related to potential constraints imposed by the Stark Law and the Anti-Kickback Statute. "We strongly encourage Congress to evaluate an amendment to these laws specifically for cybersecurity software that would allow healthcare organizations the ability to assist physicians in the acquisition of this technology, through either donation or subsidy. A regulatory exception to the Stark Law and a safe harbor to the Anti-Kickback Statute to protect certain donations of electronic health records (EHRs) effectively addresses management of technology between healthcare entities and serves as a perfect template for an analogous cybersecurity provision," the report says. "Physician groups confront myriad financial challenges. Often, these financial constraints limit their ability to manage the EHR software without trained security professionals who have the expertise to provide sufficient cybersecurity programs to protect their patient records. We need to empower small providers or suppliers (e.g., physician practices) to actively manage their security posture, not hinder them. Often, organizations want to provide technology to ensure smaller business partners do not become a liability in the supply chain. An exception may provide for this assistance without creating fear of violating the Stark Law or Anti-Kickback Statute."

• **Recommendation 2.4: Require strong authentication to improve identity and access management for healthcare workers, patients, and medical devices/EHRs.**

"The delivery of healthcare is founded on the establishment of a trust relationship between and among providers and patients. The foundation of this trust is the belief and confidence in the identities of the individuals involved (providers and patients). Through strong identity and access management practices, this trust relationship should be extended to the medical devices that are used to provide patient care," the report says. "Clinicians in a hospital setting are required to access multiple computers throughout the facility repeatedly (up to 70 times per shift) as they deliver care to patients. In order to authenticate their identity so that they can perform common tasks (e.g., access a patient's medical record, order diagnostic tests, prescribe medication, etc.), a clinician typically enters his or her username and a unique password. This widely used, single-factor approach to accessing information is particularly prone to cyberattack as such passwords can be weak, stolen, and are vulnerable to external phishing attacks, malware, and social engineering threats." ■

OCR: Ransomware Can Affect HIPAA Compliance

Responding to the recent worldwide cyberattacks that affected healthcare systems, the Department of Health and Human Services' Office for Civil Rights (OCR) has issued a reminder to covered entities about HIPAA rules on security breaches.

OCR explains in its reminder what constitutes a HIPAA security incident, preparing for such an incident, and how to respond when perimeters are breached. Cybersecurity defenses are unlikely to be 100% effective, so breaches still can occur even when covered entities have extensive, multilayered security, OCR cautions.

OCR notes that there has been some confusion about what constitutes a security incident and a reportable HIPAA breach. Some healthcare organizations experienced ransomware attacks recently but failed to report those incidents to OCR or notify patients that their electronic protected health information (ePHI) may have been accessed, OCR says.

The HIPAA Security Rule (45 CFR 164.304) describes a security incident as "an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

Covered entities need to prepare for those incidents with policies and procedures that can be activated immediately following the discovery of a security incident or data breach, OCR says.

"Policies, procedures, and plans should provide a roadmap for implementing the entity's incident response capabilities," according to OCR.

The HIPAA Breach Notification Rule requirements apply following a cyberattack that results in a breach of PHI, OCR says. The HIPAA Breach Notification Rule (45 CFR 164.402) requires OCR to be notified of a breach and notifications to be sent to patients in the event of "an impermissible acquisition, access, use, or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the protected health information."

OCR's clarification is available online at: http://bit.ly/2rLYbw2. ■

Time to Get Serious About Behavioral Health Safety in the ED

By Monica Cooke, BSN, MA, RNC, CPHQ, CPHRM, FASHRM
Quality Plus Solutions, LLC

EDs have rapidly become the primary care providers for persons with behavioral health or substance abuse disorders. The 2011 Healthcare Cost and Utilization Project (HCUP) Nationwide Emergency Department Sample (NEDS), recently published by the Agency for Healthcare Research and Quality (AHRQ), reports that 5.5 million, or 4%, of all ED visits were for a behavioral health/substance abuse diagnosis.[1]

Even more significantly, 43 million, or 33%, of all ED patients presented with either a primary or secondary behavioral health/substance abuse diagnosis. This indicates that one in three ED visits involve a patient with a significant behavioral health condition. Because of dwindling community resources and fewer inpatient treatment settings, the ED has become the "de facto" care provider for the mentally ill.

Caring for behavioral health patients often affects timely throughput of all patients in the ED and they present many other risks in the emergency care setting. The future of rapid improvement in access to appropriate treatment settings and care providers is uncertain. Therefore, organizations must identify and implement strategies to mitigate risk and improve patient safety.

The major high-risk conditions for EDs caring for behavioral health patients include suicidality, aggression, and elopement. Adverse outcomes involving behavioral conditions have led to legal claims, with the most frequent allegations including inadequate risk assessments, lack of a safe treatment environment, and lack of staff competencies. These deficiencies can lead to a variety of exposures such as regulatory risk, healthcare professional liability risk, and reputational risk from adverse media attention — none of which will fare well for organizations.

BECAUSE OF DWINDLING COMMUNITY RESOURCES AND FEWER INPATIENT TREATMENT SETTINGS, THE ED HAS BECOME THE "DE FACTO" CARE PROVIDER FOR THE MENTALLY ILL.

It is not an impossible challenge for EDs to provide safe care to the behavioral health patient population. The first step in identifying risk is to assess of the treatment setting. Once completed, this assessment can yield valuable information to set priorities for improvements and develop strategies to improve safe care and prevent adverse events.

The following are three common risk assessment findings that are high liability areas ripe for risk mitigation strategies.

1. Insufficient initial and routine assessment for patients that demonstrate high-risk behaviors. The lack of screening, assessment, reassessment, and documentation of such opens the door to liability for the facility.

Risk management strategies include the following:

- Identify patients at risk during the initial triage assessment to be followed by a comprehensive assessment by a behavioral health clinician. The identification of individual risk factors and protective factors is an important part of the assessment.
- Implement frequent assessment (every one to two hours) and document patient contact by care providers. Note: Anxiety/agitation are usually the first signs of increasing risk, and regular contact with staff helps to minimize this symptom.
- Perform reassessment at critical junctures and transitions in care: change in level of functioning, change in observation level, and at discharge.
- Assign the appropriate level of observation to the patient based on the risk assessment. Staff providing the monitoring should have documented competencies to provide this monitoring.
- Based on the risk assessment, medication management should be instituted promptly to manage symptoms. The Substance Abuse and Mental Health Services Administration (SAMHSA) has developed the Suicide Assessment Five-step Evaluation and Triage —

SAFE-T — assessment, as well. This tool could be used by professionals with limited competencies in suicide risk assessment. There also are many tools that are widely used to both screen and assess behavioral patients. While these tools can be helpful, it must be remembered that it is not possible to predict suicide.[2,3]

2. The lack of a safe treatment setting. Given the high rate of behavioral health patients presenting to EDs, it is essential that there are safely designed treatment areas to minimize the risk of suicide, aggression, and elopement. Agencies and accreditation bodies have provided recommendations for safe treatment environments, such as The Joint Commission *Sentinel Event Alert* Issue 56, which provides recommendations for the assessment and management of behavioral health patients in non-behavioral health settings and is a useful reference.[4]

Risk management strategies include the following:

• Staff should escort patients presenting with a behavioral health complaint directly into the ED or other safe location where they can be observed. High-risk patients should not be left in the waiting room, as this can increase anxiety and can lead to agitation and/or elopement.

• Conduct an initial search of the patient for any items of potential harm. These items should be secured in a locked cabinet in the room or another safe location.

• Establish "safe" rooms close to the central nursing station and not near exits or areas that provide for easy egress, such as ambulance bays. These rooms can be a permanent design, or used for other purposes and able to be converted for use as needed. The Facilities Guideline Institute published the Behavioral Health Design Guide, which is currently considered the standard in the industry for a safe environment of care.[5]

• Design a large room for two or more patients and provide recliners instead of beds for patient comfort. This can optimize staff resources for observation of patients as well.

• Provide diversions such as a television, magazines, music, food, and drinks. Doing so can decrease the patient's anxiety, and decrease risk.

• Conduct routine surveillance and searches of the designated treatment area for potentially dangerous items, such as plastic bags, sharps, ropes, and strings.

• Ensure that the bathroom used by patients is safely designed or provides for constant supervision of high-risk patients. Patients that are high risk should be constantly monitored, even when using the restroom.

• Consider the use of a different color gown, scrubs, or footies for easy identification of behavioral health patients or those at risk for elopement.

3. Insufficient staff competencies. Considering that the ED often is the first stop for patients experiencing a behavioral health crisis, it is imperative that the staff treating them know how to manage patients' behaviors and symptoms in a safe, therapeutic manner.

Risk management strategies include the following:

• Provide education/training in assessment, de-escalation, and nonviolent management of aggressive behaviors. Minimally, the staff that should be trained include security personnel, ED nursing staff, behavioral health staff, and nurse supervisors.

• Ensure that all staff involved in restraint and seclusion procedures have firm knowledge of the federal guidelines surrounding the use of these restrictive interventions.

• Provide adequate behavioral health professional support to allow for timely and comprehensive assessment. Crisis counselors, social workers, or advanced practice nurses are invaluable to assist in assessment and discharge planning. Psychiatrist consultation also should be available for evaluation if necessary.

• Hire trained behavioral health technicians to provide routine monitoring and management of behavioral patients in the ED or on units where there is a significant number of patients at any time. These staff members can be cross-trained to function as ED technicians or assistants should the volume of behavioral health patients diminish.

• Provide patient companions, or "sitters," that function as observers. These staff should have documented competencies to perform this role. The use of safety companions is widespread in acute care settings. While it is considered to be the highest level of monitoring for an at-risk behavioral patient, there is no evidence to suggest that they prevent adverse events.

• Telepsychiatry can be useful in providing timely assessment and disposition of patients. Currently, there are barriers that exist for the widespread use of telepsychiatry, including reimbursement, clinician licensing, and credentialing.

Safer care is possible for behavioral health patients in the ED. While there are many additional risk mitigation strategies that have proved to be beneficial, an organizational focus on these three high-risk areas in the management of this population can greatly assist in reducing organizational risk and improving patient safety. ■

REFERENCES

1. Healthcare Cost and Utilization Project. Overview of the Nationwide Emergency Department Sample (NEDS). Agency for Healthcare Research and Quality. Available at: http://bit.ly/2rn6Nuo.
2. Jayaram G, Herzog A. SAFE-MD: Practical Applications and Approaches to Safe Psychiatric Practice. Committee on Patient Safety, June 2008.
3. Substance Abuse and Mental Health Services Administration. SAFE-T: Suicide Assessment Five-step Evaluation and Triage. Available at: http://bit.ly/2thjenN.
4. The Joint Commission. *Sentinel Event Alert* 56: Detecting and treating suicide ideation in all settings. Available at: http://bit.ly/2sjz6sH.
5. Hunt J, Sine D. Design Guide for the Built Environment of Behavioral Health Facilities, 7.2 edition, March 2017. Available at: http://bit.ly/2rWtxjd.

HIPAA Misconceptions Still Plague Healthcare Providers

Even after years of living with HIPAA and its many requirements, healthcare providers still labor under misconceptions that could lead to noncompliance penalties, says **Gary Nelson**, healthcare practice leader of Schellman & Company, a security and privacy compliance assessor in Tampa, FL.

"Odds are that you have probably encountered a healthcare provider with a sign referring to the rules they must follow for 'HIPPA regulations,'" Nelson says. "H-I-P-P-A instead of H-I-P-A-A. It's usually a safe bet that if the individuals responsible for a provider's healthcare compliance have not read the regulations closely enough to use the correct acronym, there's a pretty good chance that there are some misunderstandings in how to apply the regulations to their practice or organization."

Nelson cites the following most common HIPAA misconceptions:

1. We're not a covered entity or health information exchange (HIE), so HIPAA doesn't apply to us.

Although the numbers are declining, some business associates still are unaware that the Omnibus Rule revised many of the administrative, technical, and physical safeguards to apply to both covered entities and business associates.

2. The software we use is HIPAA-compliant, so we're covered.

The use of software, regardless if it is developed to be "HIPAA-compliant," comprises only a small fraction of safeguards required for the security, privacy, and breach notification aspects of HIPAA and HITECH, Nelson says. A covered entity or business associate must also implement sound processes and controls around the software to address compliance gaps.

> "ODDS ARE THAT YOU HAVE PROBABLY ENCOUNTERED A HEALTHCARE PROVIDER WITH A SIGN REFERRING TO THE RULES THEY MUST FOLLOW FOR 'HIPPA REGULATIONS' — H-I-P-P-A INSTEAD OF H-I-P-A-A."

3. We are paper-based, so HIPAA doesn't apply to us.

While it is true that the HIPAA Security Rule applies only to electronic protected health information (ePHI), the HIPAA Privacy Rule still requires organizations to instill privacy processes, disclosures, and controls for the purpose of protecting patient data.

4. We can't afford to become HIPAA compliant.

A quick review of the civil penalties for noncompliance with HIPAA data breach safeguards will indicate that an organization can't afford to not become HIPAA compliant, Nelson says. "Yes, a HIPAA attestation or HIPAA compliance examination will be a cost for any organization, but it should be regarded as an investment cost to help avoid the risk of being hit with a penalty that can quickly become a six-figure, or even seven-figure violation," he says. ■

SOURCE

- Gary Nelson, Healthcare Practice Leader, Schellman & Company, Tampa, FL. Telephone: (866) 254-0000.

EMR Faults Can Be Major Factors in Med/Mal Cases

As useful as electronic medical records (EMRs) can be and as much as they can improve patient safety, they also can pose significant liability risks if they inadvertently introduce errors or make the record difficult to understand, medical malpractice attorneys caution.

Some of the features meant to make recordkeeping faster and easier actually introduce errors and muddle the facts, says **David Richman**, JD, partner with the law firm of Rivkin Radler in Uniondale, NY. He currently is working with a pain management group that was an early adopter of EMRs six years ago, and the earlier versions of the software had significant bugs that affected how clinicians filled out fields and responded to prompts for information, he says.

The latest versions of the software has been improved, but he says EMRs still create problems that might not have existed with paper records.

"We're still seeing it, and it's a pain for the providers and it's a pain for us in defending them," he says. "Even in the slightly more advanced state of today, the software is still not user friendly. I just met with a doctor two days ago discussing a malpractice case, and because of the EMR the chart has become almost unreadable."

Richman says he has seen the same problem with various EMR software packages. The problem, he explains, is that the clinician fills in the fields on a first patient visit, and on each subsequent visit the EMR autofills those fields with the same information. That may save time and effort with information that does not change often, like a patient's phone number or address, but it wreaks havoc when applied to important clinical information.

Data can be carried forth so much that the record becomes practically unreadable, he says.

"It will cut-and-paste the entire first note into the box for the second day's note. So, then you write the second day's note under that, and it carries forth all of that to the box for the third day's note," Richman says. "By day three or four, you cannot find what you are looking for because there are blocks of text just repeated over and over. Instead of picking up a doctor's traditional handwritten note where there's a date and a single entry, now doctors will spend several minutes trying to find their own notes in all that repeated information. That can't be good for medical care, and it's certainly not good when an attorney is trying to read it and figure out what happened."

Multiple Notes Needed Sometimes

EMR software also can inadvertently give the impression that a clinician was improperly tampering with or trying to alter the medical record, Richman says. Most EMRs lock down a note once it is entered, preventing the author from correcting any mistakes or omissions once it is submitted. That is meant to prevent improper alteration of notes, but then the clinician's only recourse is to enter an additional note.

"I've had records pulled for cases where the doctor has multiple versions of the same note in the file, because they reflect some change in the physician's thinking or an update in the facts as treatment goes along. I've had cases with nine or 10 versions of the same note, and those cases had to be settled, even if you can explain each version of the note and why it was entered," he says. "The more something has to be explained, the bigger problem you have. You're no longer explaining the facts of the medical care and you're trying to explain away what looks at first glance like the doctor was trying to cover his tracks. Those cases are settled purely because of the software and not because of the treatment rendered."

Other problems can arise if the EMR limits how much information can be entered in a field, he says. It is difficult for a physician to explain that he or she wanted to include more detail about a patient's condition and care, but was limited

EXECUTIVE SUMMARY

Electronic medical records (EMRs) can complicate medical records and create false impressions in a malpractice case. Autofill and the inability to edit notes can cause unexpected problems.

- Records can become cumbersome when too much information is carried forward at each visit.
- Clinicians may enter multiple notes because they cannot edit.
- Cases may be settled when EMR provides a misleading picture.

to a certain number of characters, Richman says.

An example of how EMRs affected a case of a baby with brain damage comes from **Monte James**, JD, partner with the law firm of Jackson Walker in Austin, TX. The principal allegation was that the OB/GYN miscalculated the initial due date. That OB/GYN's medical record was sent to the hospital, and the alleged incorrect due date was entered in the hospital records. The mother was thereafter admitted several times to the hospital and discharged after it was determined that she was not in labor.

For each new admission, the medical record created for that admission would auto-populate the alleged incorrect due date. The plaintiff alleged that this caused the nursing staff at the hospital to rely on an incorrect due date, and therefore fail to take appropriate action that would have otherwise been taken had the correct due date been used.

"Do not allow auto-populate features to re-input critical tests, margins, and other values such as a due date, where such results can have significant impact on the future diagnoses, care, or treatment of a patient," James says. ■

SOURCES

- **Monte James**, Partner, Jackson Walker, Austin, TX. Telephone: (512) 236-2066. Email: mjames@jw.com.
- **David Richman**, JD, Partner, Rivkin Radler, Uniondale, NY. Telephone: (516) 357-3120.

Risk Management Emerging as Credit Strength

Nonprofit hospitals are focused on risk management as a crucial variable in financial analyses and an increasingly important credit strength, Moody's Investors Service says in a new report.

The report, "Not-for-Profit and Public Healthcare — U.S.: Risk Management Crucial to Success Amid Changing Healthcare Landscape," says key areas of risk management include new IT and cybersecurity systems, clinical quality and brand protection, balance sheet health, and reimbursement.

Moody's gives the industry a poor grade overall in preventing and adequately responding to cyberattacks. Hospitals aren't spending enough of their budget on IT security but are beginning to dedicate more resources, the report says.

Accounting for roughly 25-35% of a hospital's overall capital budget, IT systems provide benefits in customer service and patient outcomes as well as potential hazards with cost overruns. Risk can arise during installation, optimization, and maintenance, while the launch might result in a temporary spike in expenses, the report notes. Guarding against cyberattacks is another area of concern.

Moody's says a hospital's ability to improve quality of care and the patient experience will increasingly affect its financial performance.

MOODY'S GIVES THE INDUSTRY A POOR GRADE OVERALL IN PREVENTING AND ADEQUATELY RESPONDING TO CYBERATTACKS.

Strategies to maintain high clinical quality involve recruiting and retaining top physician and nursing staff as well as investing in clinical technology and IT integration, Moody's Vice President **Brad Spielman** said in a statement announcing the report.

"The relationship between quality of care and operating margins is increasingly linked. The perception of poor quality or management can have a lasting negative impact on an organization's brand and patient demand, and adversely affect profitability," he said.

A healthy balance sheet provides a hospital with a buffer against unexpected liquidity demands and is a strong measure to credit quality, the report says, and there has been a general strengthening of balance sheets in recent years, with median days cash on hand for Moody's-rated portfolio increasing to 212 in 2015 from 164 days in 2010. In 2015, median days cash on hand for Aa-rated credits was 277, while the median for Baa-rated credits was 161.

Hospitals also face financial risk with the Affordable Care Act's shift toward pay-for-performance reimbursement models associated with patient outcomes. Hospitals will have to take on more risks by building in-house capabilities to manage them, the report says. The risks are inherent with both traditional insurers and the growing number of plans owned by hospitals, it says.

The report is available online at: http://bit.ly/2sl6e3x. ■

Health System Included PHI in Press Release, OCR Says

Memorial Hermann Health System (MHHS) in Houston has agreed to pay $2.4 million to the U.S. Department of Health and Human Services (HHS) and adopt a comprehensive corrective action plan to settle potential HIPAA violations related to claims it included a patient's protected health information (PHI) in a press release.

In September 2015, a patient at one of MHHS's clinics presented an allegedly fraudulent identification card to office staff, OCR reports. The staff immediately alerted appropriate authorities of the incident, and the patient was arrested. This disclosure of PHI to law enforcement was permitted under the HIPAA rules, OCR notes, but MHHS subsequently published a press release concerning the incident that included the patient's PHI.

MHHS senior management approved the impermissible disclosure of the patient's PHI by adding the patient's name in the title of the press release, OCR reports. In addition, MHHS failed to timely document the sanctioning of its workforce members for impermissibly disclosing the patient's information, OCR Director **Roger Severino** said in a statement announcing the settlement.

"Senior management should have known that disclosing a patient's name on the title of a press release was a clear HIPAA privacy violation that would induce a swift OCR response," Severino says. "This case reminds us that organizations can readily cooperate with law enforcement without violating HIPAA, but that they must nevertheless continue to protect patient privacy when making statements to the public and elsewhere."

In addition to a $2.4 million monetary settlement, a corrective action plan requires MHHS to update its policies and procedures on safeguarding PHI from impermissible uses and disclosures and to train its workforce members. The corrective action plan also requires all MHHS facilities to attest to their understanding of permissible uses and disclosures of PHI, including disclosures to the media. ■

$18 Million to Settle Kickback Claims of Loans for Referrals

Indiana University Health (IU Health), the state's largest health system, and HealthNet, an IU Health affiliate that serves low-income patients, have agreed to pay $18 million to resolve claims they engaged in a kickback scheme that involved IU Health paying for the referral of OB/GYN patients to IU Health's Methodist Hospital.

Under the settlement agreement, IU Health and HealthNet each will pay approximately $5.1 million to the United States and $3.9 million to Indiana, the Department of Justice of announced recently.

The Anti-Kickback Statute prohibits, among other things, the knowing and willful payment of any remuneration to induce the referral of services or items that are paid for by a federal healthcare program, such as Medicaid. Claims submitted to federal healthcare programs in violation of the Anti-Kickback Statute also are false claims under the False Claims Act.

Federal prosecutors alleged that from May 1, 2013, through Aug. 30, 2016, IU Health provided HealthNet with an interest-free line of credit, the balance of which consistently exceeded $10 million. The government further alleged that HealthNet was not expected to repay a substantial portion of this loan and that this financial arrangement was intended to induce HealthNet to refer its OB/GYN patients to IU Health's Methodist Hospital.

The settlement resolves a lawsuit filed in federal court in Indianapolis under the qui tam provisions of the False Claims Act, which permit private individuals to bring a lawsuit on behalf of the United States for false claims and to share in any recovery. The lawsuit was filed by Judith Robinson, MD, who formerly held several positions at both Methodist Hospital and HealthNet. Under the settlement, Robinson will receive approximately $2.8 million out of the federal share of the recovery. ■

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. Go to "My Account" to view your available CE activities. First-time users must register on the site using the subscriber number printed on their mailing label, invoice, or renewal notice.
3. Pass the online tests with a score of 100%; you will be allowed to answer the questions as many times as needed.
4. After successfully completing the test, a credit letter will be emailed to you instantly.
5. Twice yearly after the test, your browser will be automatically directed to the activity evaluation form, which must be completed to receive your credit letter.

CME/CE QUESTIONS

1. **Regarding the WannaCry cyberattack, what does Marc S. Voses say about the target of the attack?**

   a. Healthcare organizations were not a particular target, but were vulnerable because tight budgets left them with poor security.
   b. Healthcare organizations were one of several specific targets that included military installations and financial institutions.
   c. Healthcare organizations were not a particular target and were among the least affected because they tend to have better cybersecurity.
   d. Healthcare organizations were the primary target, and most were not affected because they had good cybersecurity.

2. **How does a ransomware attack work?**

   a. Hackers threaten to access an organization's computer system unless payment is made to prevent the attack.
   b. Hackers access an organization's computer system and encrypt it, then demand ransom to unencrypt the data.
   c. Hackers steal data from an organization and threaten to publish it unless payment is made.
   d. Hackers steal data from an organization and publish it, then demand payment to take the information off the internet.

3. **What does Monica Cooke recommend regarding high-risk behavioral health patients?**

   a. They should wait in the general ED waiting room like everyone else.
   b. They should not wait in the general ED waiting room because that can worsen anxiety.
   c. They should be seen as quickly as possible regardless of the triage process.
   d. They should be escorted directly to a behavioral health unit for evaluation, rather than being seen in the ED.

4. **What is one flaw in electronic medical record software cited by David Richman, JD?**

   a. The record autofills and carries forward too much information from one patient visit to the next.
   b. The record does not autofill and carry forward enough information from one patient visit to the next.
   c. The record often converts numerical values incorrectly.
   d. The record fails to prompt clinicians for the necessary input.

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

Failure to Monitor Medication During Birth Leads to $14.5 Million Verdict

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

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

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

News: In 2012, a 24-year-old woman went to a hospital to give birth. A procedure was performed, which revealed a stool from the baby in the amniotic fluid. The physician ordered a high dose of a natural contraction-producing hormone to increase contractions. Throughout the birthing process, this hormone was continuously administered in a high dose without monitoring.

The baby's vital signs revealed potential acidosis, and the baby eventually was delivered with severe brain damage. He required intubation and suffered a seizure shortly thereafter. As a result, the family brought a medical malpractice suit against the physician, the hospital, and the hospital's parent company, alleging that the failure to monitor the hormone and the labor caused the child's birth defects. The case proceeded to a lengthy trial that culminated in a jury award of $14.5 million for the family.

Background: On July 19, 2012, a woman presented to a hospital for the delivery of her son. At 6:30 p.m., the mother was examined by an OB/GYN, who performed an artificial rupture of membranes (amniotomy), which revealed thick meconium (an infant's earliest stool, and here an indication of fetal stress). The physician informed the pediatrician of the thick meconium and ordered a high dose of Pitocin, a natural hormone, to increase the strength and frequency of contractions.

At 7:10 p.m., the OB/GYN determined that the patient was fully dilated and instructed her to start pushing in the second stage of labor, with the Pitocin still running. Then, at 8:00 p.m., the physician attempted to turn the face-up fetus to expedite delivery. By this point, the fetal heart rate revealed minimal variability, an indication of fetal acidosis due to a restriction of the baby's oxygen flow.

THE BABY'S VITAL SIGNS REVEALED POTENTIAL ACIDOSIS, AND THE BABY EVENTUALLY WAS DELIVERED WITH SEVERE BRAIN DAMAGE.

By 8:20 p.m., the baby's head was crowning, and the physician later claimed this meant the baby could have been delivered by vacuum or forceps. At 8:25 p.m., the fetal heart rate slowed dramatically to 60 beats per minute (bradycardia). To try to give the fetus time to recover, the physician instructed the mother to lay on her side and had her breathe through a contraction without pushing. Throughout this process, the Pitocin continued running. The physician then performed an episiotomy, and the baby was born unresponsive at 8:31 p.m. with his vital signs severely depressed. The child's Apgar scores were 2, 2, and 3, taken the first, fifth, and 10th minute after birth, respectively. Scores of 7-10 are considered normal. He was intubated and suffered seizures and severe brain damage.

The child later was diagnosed with spastic tetraplegic cerebral palsy and required treatment from various medical specialists, including an orthopedist, a neurologist, and a gastroenterologist (as he likely would need a feeding tube for nutrition). He was treated with

physical, occupational, and speech therapies. He will require lifelong treatment, including medications to treat spasticity and seizure disorder, radiographic imaging, physical therapy, and constant monitoring by a pediatrician or primary care physician, neurologist, gastroenterologist, urologist, orthopedic surgeon, and neuro-ophthalmologist.

The baby's parents sued the OB/GYN and the hospital, alleging that their negligence breached the standard of care and constituted medical malpractice. The plaintiffs claimed that the use of Pitocin was improper and that the physician and nursing staff failed to properly monitor the labor.

At trial, eight experts with specialties in OB/GYN, neonatology, physical medicine, and life care planning testified for the plaintiff. The obstetrics experts opined that the use of Pitocin was improper and that before it was used, the fetal heart rate was indicative of a healthy baby. Furthermore, the physician and nursing staff failed to turn off the hormone when the baby experienced fetal distress from the frequency of contractions and lack of time to recover, subjecting the baby to 40 minutes of severe hypoxia and acidosis, and ultimately causing permanent brain damage.

One of the defense's five experts testified that the hospital's nursing policy prohibited starting the mother on Pitocin because her contractions were too frequent, and that its administration should have ceased when the fetal heart rate was concerning.

When the physician testified, he stated that under his custom and practice, he would have turned off the Pitocin between 7:55 and 8:00 p.m. The physician also stated he believed he gave the nurse such an order, but that was not reflected in the medical record, and the nurse denied receiving the order.

The jury returned a verdict in favor of the plaintiffs for just under $14.5 million after a nine-day trial. The jury found the physician 60% liable and the hospital 40% liable.

What this means to you: This case shows the double-edged sword of internal operating procedures. The procedures can be helpful in insulating hospitals from liability, but they also provide a peg on which plaintiff's counsel can hang their hats when it comes to a physician's deviation from the standard of care. Of course, limiting liability wherever possible certainly is advisable, but hospitals also should take into consideration the extent to which their internal procedures expose medical professionals to malpractice claims. Hospitals may consider prioritizing restatements of law in drafting their procedures. For example, an internal procedure that requires physicians and nurses to obtain informed consent is simply a restatement of the law, and it helps to insulate the hospital from liability by providing something the defense counsel can point to at trial. Such an internal procedure would carry less weight for the plaintiff in a case against a physician than would a more specific procedure. For example, if in this case the hospital issued an internal procedure that specifically required physicians to cease hormonal treatments when fetal vitals drop below a certain point, the plaintiff in this case would have had more powerful evidence to work with.

That said, the other side of the double-edged sword is the notion that too general a set of internal procedures may result in physicians operating outside the standard of care due to their ignorance of the standard. This means that hospitals should ensure that physicians understand very well what the standard of care may be in any given situation. This tension between preventing liability for hospitals and preventing injuries to the extent permitted by human error should be considered by those responsible for drafting internal procedures, and hospitals and medical professionals should work closely with counsel in drafting internal procedures.

Note also that in this case, the nursing policy on the use of Pitocin would have been approved by the medical staff of the obstetrics department, and the physician and nurse should have followed it. Had the physician ordered the Pitocin despite what is stated in the policy, the nurse should question the physician as to the reason. The nurse has the responsibility to activate the chain of command if the explanation is not reasonable to the nurse. Both the nurse and physician have been trained to monitor and interpret fetal monitoring strips that should run continuously throughout the entire labor. Interpretation of the strips, including the variability of the fetal heart rate during and after contractions, is critical even during uneventful labor, and discussions of the results should occur frequently and between all healthcare professionals in the delivery room. Communication among all involved is critical.

Finally, ensuring that the medical records are completely accurate provides credibility at trial. Medical professionals should strive to create clear and consistent records, to the extent possible, that they can fall back on in a legal setting. One challenge is preserving those

records over the long period of time required to fully litigate a case. Most hospitals hold on to perinatal records for 10 years due to damages that show up as a child grows. There are many companies that offer medical record storage services and can be used to authenticate records and bolster their credibility. Hospitals and medical professionals should consider working with one or more such companies if they are not doing so already. ■

REFERENCE

Decided on Jan. 27, 2017, in United States District Court, W.D. Pennsylvania, Case No. 14CV00149.

Hospital and Physician Prevail on Medical Negligence/Wrongful Death Appeal

News: A California court of appeals recently upheld a motion for summary judgment in a case involving the death of a child during birth. The decedent child was born in 2011 at a California hospital. The child was born unresponsive and was transferred to a neonatal ICU. After several months of testing and treatment, the child passed away due to a brain injury that occurred before the transfer to the NICU.

The family sued the hospital that operated the NICU and the physician, alleging medical malpractice, negligent infliction of emotional distress, and wrongful death. The defense brought a summary judgment motion, which was granted by the trial court. Despite some creative arguments by the plaintiff on appeal, the appeals court held in favor of the defendants, upholding the grant of the summary judgment motion.

Background: On Sept. 27, 2011, at 12:17 p.m., the decedent child was born at a California hospital. She was cared for and underwent testing at the hospital by nurses who communicated with the attending physician-pediatrician. The following morning, the baby was unresponsive and was then transferred to the NICU, a unit housed by the first hospital but operated by another hospital. At the time of transfer, the child was noted to have no heart rate or respiratory rate.

The neonatologist at NICU did not care for the decedent, nor was he consulted prior to her arrival at NICU. Until her arrival, the baby was under the care of the Fresno physician-pediatrician. The NICU neonatologist was a member of a neonatology physicians group and was responsible for providing care and treatment to patients in NICU. None of the nurses or staff for the first hospital aided the NICU.

When the baby was transferred to the NICU, the neonatologist took over ventilation with a bag mask and intubated her using an endotracheal tube. She was connected to an intravenous line and underwent further testing. Unfortunately, the baby died on June 18, 2012. It was later determined that the child died of complications resulting from a hypoxic brain injury that occurred on Sept. 28, 2011, before she was brought to the NICU physician for resuscitation.

The decedent's parents filed suit against the neonatologist and the first hospital, alleging medical malpractice, negligent infliction of emotional distress, and wrongful death. None of the treating physicians were agents or employees of the first hospital. The defendants brought a motion for summary judgment in which the neonatologist proffered expert testimony from a physician who concluded that he did not deviate from the standard of care and that his treatment was not the cause of the baby's death. The hospital offered testimony from a registered nurse and physician who provided similar opinions.

The plaintiff opposed the summary judgment motion and offered the declaration of an expert who stated that both defendants breached their respective standards of care. The defendants entered objections to the plaintiff's expert declaration, which were sustained. As a result, the court entered summary judgment in favor of the defendants.

On appeal, the plaintiff argued that his expert used in opposition to the motion for summary judgment had adequate factual foundation for his expert opinion, and the trial court's entry of summary judgment was error. The defense maintained its position that neither defendant was liable for negligence causing the unfortunate death of the child. The defense stressed that the hospital and NICU are distinct, separate entities, that the neonatologist did not care for the child until her transfer to NICU, and that the first hospital's physician-pediatrician did not criticize the degree of care exercised by the neonatologist while treating the child.

The petitioner-plaintiff failed to comply with a local rule that requires parties to cite directly to the record or risk waiver of their factual contentions. As a result, the court of appeals deemed some of the petitioner's arguments as waived. Furthermore, the petitioner failed to designate his expert witness declaration as part of the record, resulting in a record without expert evidence for the petitioner. Finally, the court held that the foundation on which the expert's testimony relied was insufficient. The trial court's summary judgment was ultimately affirmed by the court of appeals.

What this means to you: The admissibility of an expert witness report was the crux of this case. Medical malpractice cases typically require more expert witness testimony than many other areas of practice. As such, a strong understanding of the applicable rules of evidence, especially as to experts, is imperative for a favorable adjudication. The court of appeal noted that the petitioner's expert was qualified, but the deficiency was in the foundation laid for his testimony. This raises two issues in the defense of medical malpractice cases: the requirement that experts be qualified under requirements applicable to experts, and the prohibition of conclusory testimony.

As to establishing an adequate foundation, first and foremost, facts must be preserved in the appellate record. At the trial level, the plaintiff's expert opined that the hospital's nurses should have diagnosed the case as a high-risk pregnancy and consulted a neonatologist early. The defense objected to this in part because the hospital that would have made such a determination was not a named defendant in the suit. The appeals court noted that the nurses involved in the case would not have the authority nor the duty to characterize the pregnancy as high-risk while it was assigned to a physician. However, attorneys frequently argue that while it is beyond the scope of practice for the registered nurse to diagnose, it is well within his or her scope to question the practice of the physician and initiate the chain of command if he or she becomes aware of an unusual order or practice that appears to breach the standard of care. In any event, to lay a factual foundation for an expert, one must develop an in-depth understanding of the facts of the case and competently set them forth with appropriate evidence. Courts are the gatekeepers of expert testimony, as well as other forms of evidence, and take that role seriously.

From the appeals court's opinion, it is unclear why the plaintiff did not join the first hospital and physician-pediatrician. Failing to do so appears to have been a fatal flaw for the plaintiff, especially considering the defense's emphasis on the separation of ownership between the hospital and NICU. It is possible that the testing and resuscitation attempts at the NICU occurred while the statute of limitations ran on any claims against the first hospital, and the limitation period expired by the time the plaintiff sued. Statutes of limitation usually are relatively short in medical malpractice cases, but many jurisdictions do use a discovery rule for the accrual of a cause of action — delaying the running of the statute of limitations until the plaintiff discovers or should reasonably discover the injury. Therefore, it behooves medical professionals and hospitals to make careful note of when a plaintiff's statute of limitations begins and expires.

Most hospitals with a NICU maintain an emergency response team, similar to Rapid Response or Code Blue teams, that can be called to the delivery room at the first sign of fetal distress during birth. That way, critical interventions such as suctioning, airway maintenance, and resuscitation can be performed immediately, thus avoiding transportation delays to another part of the hospital. The neonatologist, if required, also could be called to the delivery room by the NICU response team. A contractual agreement between the hospital and the NICU that included a credentialing agreement between the medical staffs would have allowed this scenario.

Finally, the defense in this case faced a difficult set of facts that carried a risk that a jury may render a verdict based on the emotions elicited from the fact that a child died rather than based on the legal principles involved. For that reason, success pretrial was crucial. The attorneys for the defense in this case exhibited mastery of the Federal Rules of Evidence and were diligent with local rules. Their objections were pointed and well-taken by both courts. As a result, the attorneys were rewarded with a pretrial ruling in their client's favor and an affirmation by the court of appeal. Hospitals and medical professionals should work closely with counsel from the start of the case and throughout the case to develop sufficient evidence during pretrial discovery to win the case on motions practice prior to trial, as medical malpractice cases almost always lend themselves to emotionally charged facts that will appeal to juror sympathies at trial. ■

REFERENCE

Decided on March 16, 2017, in Court of Appeal of California, Case No. F072414.