ED LEGAL LETTER™

THE ESSENTIAL RESOURCE FOR EMERGENCY MEDICINE MALPRACTICE PREVENTION AND RISK MANAGEMENT

APRIL 2016 Vol. 27, No. 4; p. 37-48

INSIDE

Hackers Target Hospitals with "Ransomware"

Is your ED prepared?

A recent "ransomware" cyberattack at Hollywood Presbyterian Medical Center in Los Angeles left clinicians unable to access patient medical records for 10 days in February until the hospital paid hackers a $17,000 ransom in bitcoin. The FBI is currently investigating the attack.

A hospital spokesperson declined to comment on the incident when contacted by *ED Legal Letter* for this story. In an official statement, the hospital's president and CEO said, "The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this."

Raj Mehta, a partner at Deloitte & Touche's Cyber Risk Services practice, has seen a sharp increase in targeted cyberattacks against healthcare providers.

"Who would have thought several years ago that you could affect healthcare operations, and potentially patient safety, through a cyberattack?" he asks.

Cyberattacks against doctors and hospitals have more than doubled in the past five years, with the average data breach costing a hospital $2.1 million, according to a May 2015 study from the Ponemon Institute, a security research and consulting firm. (The Fifth Annual Study on Privacy & Security of Healthcare Data is available at www2.idexpertscorp.com/ponemon.) Other key findings:

- **Nearly 90% of healthcare providers were hit by breaches in the past two years, half of them criminal in nature.**
- **Criminal attacks in healthcare are up 125% since 2010, and are now the leading cause of data breach.**

More than half of healthcare organizations don't believe their incident response process has adequate funding and resources, according to the report.

Mac McMillan, co-founder and CEO, CynergisTek, an information security and privacy consulting firm, says there was "a huge outcry" for in-

Financial Disclosure: The following individuals disclose that they have no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study: **Arthur R. Derse**, MD, JD, FACEP (Physician Editor); **Stacey Kusterbeck** (Contributing Editor); **Jonathan Springston** (Associate Managing Editor), and **Kay Ball**, RN, PhD, CNOR, FAAN, (Nurse Planner); and **Shelly Morrow Mark** (Executive Editor)

ED LEGAL LETTER

ED Legal Letter™,
ISSN 1087-7347, is published monthly by
AHC Media, LLC
One Atlanta Plaza
950 East Paces Ferry Road NE, Suite 2850
Atlanta, GA 30326.
Periodicals Postage Paid at Atlanta, GA 30304 and at additional mailing offices.

POSTMASTER: Send address changes to:
ED Legal Letter
P.O. Box 550669
Atlanta, GA 30355.

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

EDITORIAL EMAIL ADDRESS:
jonathan.springston@ahcmedia.com.

SUBSCRIPTION PRICES:
Print: 1 year with free *AMA PRA Category 1 Credits™*: $519.
Add $19.99 for shipping & handling.
Online only: 1 year (Single user) with free *AMA PRA Category 1 Credits™*: $469

Back issues: $83. Missing issues will be fulfilled by customer service free of charge when contacted within one month of the missing issue's date.
GST Registration Number: R128870672.

ACCREDITATION: AHC Media, LLC is accredited by the Accreditation Council for Continuing Medical Education to provide continuing medical education for physicians.

AHC Media, LLC designates this enduring material for a maximum of 18 *AMA PRA Category 1 Credits™*. Physicians should claim only credit commensurate with the extent of their participation in the activity. Approved by the American College of Emergency Physicians for a maximum of 18.00 hour(s) of ACEP Category I credit.

AHC Media, LLC is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation.

This activity has been approved for 18 nursing contact hours using a 60-minute contact hour. Provider approved by the California Board of Registered Nursing, Provider #CEP14749, for 18 Contact Hours.

This activity is intended for emergency physicians and nurses. It is in effect for 36 months from the date of the publication.

Opinions expressed are not necessarily those of this publication, the executive editor, or the editorial board. 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 in specific situations.

EDITORIAL/CE DIRECTOR: Lee Landenberger
EXECUTIVE EDITOR: Shelly Morrow Mark
ASSOCIATE MANAGING EDITOR: Jonathan Springston
PHYSICIAN EDITOR: Arthur R. Derse, MD, JD, FACEP
CONTRIBUTING EDITOR: Stacey Kusterbeck

formation about ransomware attacks after the Los Angeles incident. Not surprisingly, hospital executives and board members wanted to know how to avoid similar attacks.

"The reaction that we are seeing has been pretty pronounced," McMillan says. "But what if they knew how many of these events are actually occurring all the time?"

The vast majority of attacks never appear in the media.

"There are a number of attacks going on that are not so visible," Mehta says. "Healthcare is likely the number one targeted industry."

McMillan is aware of many other hospitals that were hit by ransomware attacks.

"The ones you didn't hear about are the ones who were prepared," he explains. If hospitals are unprepared to mitigate the damage of the ransomware attack, though, "chaos ensues, and the local media starts interviewing patients," McMillan adds. "That's pretty hard to hide."

Less Than 5% of IT Budget

The attack is a red flag that hospitals are underinvesting in cybersecurity, according to **Tom Kellermann**, CTO, Strategic Cyber Ventures.

"Hospitals are incredibly dependent on technology and have massive IT budgets," he says. "But they are still not investing in protecting networks from cyberattacks."

In August 2014, the FBI warned that healthcare cybersecurity systems are lax compared to the financial and retail sectors. Healthcare data is worth more money on the black market than credit card data, Mehta explains, because it can be used in multiple ways. Hackers can use it to commit identity theft, medical fraud, for extortion, or to obtain prescriptions for controlled substances.

Hospitals typically invest primarily in physical security, such as guards and cameras, with most spending less 5% of their IT budgets on cybersecurity, according to Kellermann.

"Most of the investment is focused on firewalls and encryption — outdated technology," he says. "Hospitals should immediately allocate at least 20% of their IT budgets to cybersecurity."

Damage Is Multifaceted

The ransomware attack against Hollywood Presbyterian "goes to show that as an organization, we are a single incident away from having a significant impact," says **Sanjeev Sah**, chief information security officer at Texas Children's Hospital in Houston.

Media coverage focused largely on the $17,000 ransom that was paid.

"But that's not the real cost," McMillan says. "The ransom was minimal compared to the operational cost, in terms of loss of revenue from services." With the hospital down for 10 days and diverting patients to other health systems, "that undermines confidence in the system on many levels," McMillan adds.

A secondary infection is likely to exist with ransomware attacks.

"You need to be very diligent to be sure that the network has been properly disinfected after an event," Kellermann warns. "Otherwise, you can get hit again."

Should hospitals pay the ransom? **David McHale**, senior vice president and chief legal officer, The Doctors Company, a medical malpractice insurer, says this depends on these factors:

- **the circumstances surrounding the attack**;

• **whether all, or only part, of the system has been compromised**;

• **the degree to which recovery or restoration of the system can be achieved**.

"If a hospital can fully restore its systems, then that hospital has the option to refuse to pay the ransom — and certainly will be in a better position than the hospital that does not have an electronic backup," McHale says.

The hospital would also need to consider these questions: How effective is the backup? Is the backup performed frequently enough to have full systems restored? Is the system immune to a second hack, or could the backup be compromised?

"The fact of an electronic backup is not, standing alone, the sole determining factor in whether to refuse to pay," McHale says.

What Liability Exists?

Telling patients that hospitals will care for their well-being, yet allowing a ransomware attack to harm their virtual well-being, "is not to be tolerated, in this day and age," Kellermann says.

If a patient suffers harm as a result of a cyberattack and the hospital or EP is sued, Kellermann says hospitals "have two things they can hide behind." One defense is plausible deniability — that the hospital didn't know what was going to happen. The other defense is that the data was encrypted. This is not a sufficient defense, according to Kellermann, since the hacker likely has stolen the password to unlock the encryption.

"It's like saying the suitcase was locked when someone has the key," he says.

Just as emergency physicians (EPs) protect patients from hospital-

EDs Should Make These Changes ASAP

Here are some approaches cybersecurity experts say can protect hospitals against cyberattacks.

• **Keep systems as up-to-date as possible**. **Craig Musgrave**, senior vice president of information technology, The Doctors Company, says EDs should install: intelligent firewalls to stop malware from downloading; intrusion detection software to monitor illegal activities on computer networks; and anti-virus, anti-malware, or application whitelisting software to stop malware from executing on desktop computers.

Mac McMillan says, "Antiquated, unsupported environments do not belong in a contemporary healthcare setting."

Steve King, COO, Netswitch Technology Management, says EDs should:

1. Segregate networks, so medical devices are not accessible from the administrative network;
2. Establish least-privileged access and install a privileged account management system;
3. Implement a holistic security management suite from a reputable managed security services vendor;
4. Create an off-site file back-up system.

• **Inform all users about what they can personally do to avoid letting a cyberattack into the hospital's system**. "Organizations need to understand their weaknesses — the people side of the equation — as well as the processes and technologies," says **Raj Mehta**.

Musgrave says EDs should train staff to avoid downloading, clicking on links, or running unknown USB device on computer systems.

The risks of mobile devices used by staff can't be ignored. McMillan says, "Things like phishing messages and downloading from the Web are some of the more common ways cyberattacks [occur]. If users are connecting remotely from home, what is protecting that data?"

Apparently, a single email click started the recent ransomware attack at Hospital Presbyterian Medical Center. **Sanjeev Sah** says, "We prevent many spam and phishing attempts from getting in, but not all. In this particular case, it would have been extremely helpful if the person receiving the message would have avoided that click."

Traditional annual inservices are outdated. Sah recommends ongoing, on-demand training to keep employees updated on new threats. It's also important for ED leadership to understand why certain actions are needed, such as users authenticating every time they use a device.

• **Implement a backup plan so normal operations can continue during a cyberattack**. Even the most up-to-date malware and antivirus filters can't stop every cyberattack. That's where the ED's backup plans become very important.

• **Be more objective in the way security is analyzed, by using independent third parties to perform audits and assess risk**.

• **Implement a well-tested process to respond to a cyberattack**. Drills simulating a cyberattack, as EDs do with disaster preparedness, can determine who would talk to the media, patients, and families. ■

acquired infections by washing their hands, they're also responsible for the virtual health of their patients, Kellermann stresses.

"Every time a doctor looks at an amazing new application, they should also recognize that the criminal community, and nefarious individuals, have figured out ways to get into those things," he says.

Kellermann says EPs should ask these questions of hospital administrators: Have we had any events? How much are we investing in security? How do we protect our devices? I know we are moving to the cloud, so what is our strategy for security?"

If the hackers sold patient information, the hospital would be subject to claims for damages for identity theft from its patients, investigation by the federal government, and possible fines for violations of the Health Insurance Portability and Accountability Act, McHale says.

If the hospital has confirmed that patient care was not compromised and no personal information of the patients was stolen, the hospital likely does not face much in the way of legal liability, according to McHale. However, "if patient care was compromised, the hospital could potentially face claims of professional negligence," he says.

Kellermann says the Los Angeles incident should be "a giant red flag to the community at large, that modern healthcare has been virtualized."

Hospitals are very vulnerable to cyberattacks because of the high-dollar value of healthcare records.

"Healthcare records sell for $70 a record, as opposed to $5 to $20 for credit card or financial records," Kellermann explains. "The value of healthcare records is dramatically more than any record out there, with the exception of intellectual property."

Once patients' healthcare records are sold, this leaves them open to extortion attempts or having lines of credit or equity opened in their names. Extortion campaigns against prominent physicians and patients are another possibility.

"The records have everything to allow you to understand how someone is vulnerable — including their emergency contacts, so you know who they trust — and they can be sent targeted phishing emails [that are infected with malware] accordingly," Kellermann says.

In some cases, criminal groups pay individuals with hacking expertise to create malware that targets a specific hospital.

"The criminal groups get the ransom out of the target. But the creator of the malware now has a backdoor to conduct a secondary infection," Kellermann notes.

Cybersecurity experts point to another threat: Life-support machines are becoming more complex, networked, and hackable.

"They are difficult to protect because they don't have a lot of memory and are difficult to update due to state laws that machine settings cannot be changed unless they are certified," Kellermann says.

Mobile devices and tablets used by EPs are also vulnerable to attack, putting the organization at risk of contagion. The financial sector and the government banned the practice of using the same password for all devices and public Wi-Fi. However, it is still a common practice in healthcare, Kellermann notes.

"Within the next three years, we will see a terrible event that affects the virtual health of tens of thousands of people that is traced back to a physician violating mobile security policy," Kellermann predicts. "It hasn't happened, but it's inevitable." ■

EPs' Legal Risks Post-cyberattack Are Unclear

A hospital is sued for failure to take reasonable efforts to prevent a cyberattack that harmed an ED patient. Could the emergency physician (EP) also be liable?

"This is such a new phenomenon, there is no case law to serve as a basis for litigation. The outcome of any case would be solely based on the arguments made by the opposing lawyers," says **Kevin G. Rodgers**, MD, president of the American Academy of Emergency Medicine. Rodgers is also professor of clinical emergency medicine and residency program director emeritus at Indiana University Health Methodist in Indianapolis.

Many states conduct peer review panels of potential malpractice cases before moving forward to court.

"A malpractice case clearly based on lack of patient records due to institutional failure to make them available due to cyberattack would be viewed by other EPs on the panel as a system failure," Rodgers says. "They would find in favor of the physician."

An EP does not have vicarious liability for a hospital, Rodgers emphasizes.

"The most defensible position for the EP in this scenario is that this is an institutional/system failure," he says.

In any root cause analysis conducted after an adverse event, a variety of potential causes are assessed. One of these is system failure, Rodgers notes.

"Any legal liability directly related to medical malpractice that would have been clearly prevented by having patient records available lies purely

with the institution, with the institution being solely liable," Rodgers says.

No Access to Records

For EPs, lack of access to patient records isn't unique to a cyberattack — it's something they deal with on a daily basis.

"Residency-trained, board-certified, or board-eligible emergency medicine physicians are quite adept at obtaining the required information needed to appropriately care for patients from a variety of sources," Rodgers says.

This includes calling extended-care facilities, family, other hospitals, pharmacies, or the patient's primary care provider.

"EPs commonly have to make emergent decisions on less than total information," Rodgers notes.

But what if the ED could have accessed a particular patient's records if not for a cyberattack, and something in the records would have affected the treatment provided?

If an adverse outcome occurred in this scenario, "there is a possibility that a claim for professional negligence could be asserted," according to **David McHale**, senior vice president and chief legal officer, The Doctors Company.

However, the plaintiff would have a difficult time successfully arguing that the EP should not have undertaken the emergency care until medical records of the patient could be accessed.

"This is certainly a reach," McHale says. "In many instances, an ED must treat a patient without any access to records. It's a reality of seeing patients on an emergent basis."

If records are locked by "ransomware," ED staff simply have to do the best they can under the circumstances, says **William Sullivan**, DO, JD, FACEP, an emergency physician at the University of Illinois in Chicago and a practicing attorney in Frankfort, IL. For example, patients can report allergies, which can be noted in written records. In complex patients, other facilities or primary care physicians could be contacted to fax records to the ED.

"The law requires us to act reasonably under whatever circumstances we are faced with," Sullivan explains. "Obviously, we're put at a disadvantage if we don't have a patient's old medical records."

This circumstance would change the standard to which the EP would be held.

"It would be a good idea to note on the records somewhere that old medical records were not available due to IT problems, though," Sullivan says.

If a lawsuit is filed several years later, the EP might not remember why he or she didn't have access to the old records on that particular day, and what the EP did to mitigate the situation.

EPs are trained to be more cautious and conservative in their decision making and dispositions when there is potential missing information, Rodgers adds.

"This would include more liberal admissions, longer observation periods in the ED or observation units, and arrangement of closer follow-up with primary care physicians and specialists," he says.

It is generally the hospital's duty to maintain the security of the electronic medical record (EMR), Sullivan notes.

"If there has been a data breach, then there are also rules that hospitals must follow in order to mitigate the breach," he says.

Under 45 CFR 164.404, a covered entity must notify any individual whose unsecured protected health information (PHI) has been breached, within 60 days of discovering the breach. This notification must include the nature of the breach, the type of information involved, and what steps the patients can take to protect themselves from possible harm.

If more than 500 unsecured patient records are affected, under 45 CFR 164.406 the hospital also has to notify prominent media outlets within 60 days of the discovery of the breach. In addition, under 45 CFR 164.408, all breaches of unsecured PHI must be logged and reported to the Department of Health and Human Services on at least a yearly basis.

"There are also specific penalties based on the type of breach — accidental vs willful — and how the information is used," Sullivan says.

Under 45 CFR 160.404, hospitals can be fined up to $50,000 for each violation involving "willful neglect" of privacy practices. Unauthorized access of PHI with intent to sell or transfer the data for personal gain or malicious harm can lead to fines of $250,000 and up to 10 years in prison, pursuant to 42 U.S.C. § 1320d.

There is no individual cause of action against a covered entity under the Health Insurance Portability and Accountability Act (HIPAA), says **Deborah Hiser**, JD, a partner with Husch Blackwell. The ED, as a HIPAA-covered entity, would be subject to civil penalties from the Office of Civil Rights if the patient's protected health information were unsecured as defined by the National Institute of Standards and Technology rules.

"The analysis is also dependent on the facts and how the attack occurs," Hiser says. "There are state breach of security system laws that would impose notice requirements to patients, as does HIPAA."

Hiser says liability would depend on who is responsible for security of the EMR, and whether any PHI were further used or disclosed in violation of HIPAA.

"I would not think an individual physician would be liable under a malpractice theory," she says. "This is an evolving issue. We do not yet know the extent of liability."

Sullivan sees no liability for EPs unless the EP was somehow involved in the breach. One example of when an EP could face liability is if the EP shared his or her password with others, and that password was used to breach the EMR.

"That type of breach would likely result in access to a few medical records, not in the large-scale database breach experienced by the California hospital," Sullivan notes.

If an EP accesses the EMR from home, it is possible that the EP's home computer could be compromised as well, Sullivan adds. For example, keyloggers could capture passwords that the hacker later could use to access records from another site.

"The most important point in this regard is to log off when you're done with the session and to change your password regularly," Sullivan says. "It may not prevent a breach, but will decrease the likelihood of one happening."

If the EP installs a program on a hospital computer or visits a malicious website, the program or website could install a virus or backdoor, providing hackers access to the hospital system.

"If the hospital has a policy regarding use of computers and other IT and the physician violates it, the physician could be subject to termination," Sullivan says. ■

SOURCES

- **Deborah Hiser**, JD, Partner, Husch Blackwell, Austin, TX. Phone: (512) 703-5718. Email: Deborah.Hiser@huschblackwell.com.
- David McHale, Senior Vice President, Chief Legal Officer, The Doctors Company, Napa, CA. Phone: (707) 226-0289. Fax: (707) 226-0370. Email: McHale@thedoctors.com.
- **Kevin G. Rodgers**, MD, Department of Emergency Medicine, Professor of Clinical Emergency Medicine, IU Health Methodist, Indianapolis. Phone: (317) 962-5975 Email: kgrodger@iu.edu.
- **William Sullivan**, DO, JD, Frankfort, IL. Phone: (708) 323-1015. Email: wps013@gmail.com.

Are Copays Collected in ED? Beware of EMTALA

In light of patients' higher out-of-pocket costs, registration staff are collecting from ED patients upfront instead of billing them — in some cases, co-pays or deductibles totaling hundreds of dollars. This practice could trigger an Emergency Medical Treatment and Labor Act (EMTALA) investigation, warns **Sue Dill Calloway**, RN, JD, president of Patient Safety and Healthcare Education & Consulting. Dill Calloway is also vice president of risk and patient safety at Emergency Physicians Insurance Exchange.

To minimize any EMTALA concerns, the medical screening examination and any medical care needed to stabilize an emergent medical condition should never be delayed as a result of obtaining any financial information — including collecting co-pays, says **Mark Reiter**, MD, MBA, FAAEM, residency director, University of Tennessee-Murfreesboro/Nashville. Reiter is also CEO of Emergency Excellence, an ED consulting firm.

"We would recommend that whenever a physician enters the patient room, the registration staff should excuse themselves and return later," he adds.

A hospital's obligation to screen for and stabilize an emergency medical condition cannot be influenced by whether a copay is paid or not, Reiter emphasizes.

"If no emergency medical condition is found, or if an emergency medical condition is stabilized, then a hospital has the right to insist on payment for non-emergent care," he says.

The Centers for Medicare & Medicaid Services issued a Dec. 13, 2013, surveyor memo on payer requirements and collection practices.[1]

"Hospitals cannot request payment or co-pays until after the appropriate medical screening is done and they have had stabilization treatment," Dill Calloway says.

One hospital was fined $40,000 for an incomplete medical screening examination on a patient with fever, chills, and urinary tract infection symptoms.

"The triage nurse told the patient to pay $85 before the medical screening examination, and she left," Dill Calloway says. "This should be on the radar screen of every hospital." ■

REFERENCE

1. Centers for Medicare & Medicaid Services. Emergency Medical Treatment and Labor Act (EMTALA) requirements & conflicting payor requirements or collection practices. Available at: http://go.cms.gov/1YBf585

SOURCES

- **Sue Dill Calloway**, RN, JD, Vice President, Risk and Patient Safety,

Emergency Physicians Insurance Exchange Risk Retention Group, Auburn, CA. Phone: (614) 791-1468. Email: sdill@epixrrg.com.

- **Mark Reiter**, MD, MBA, FAAEM, CEO, Emergency Excellence; Residency Director, University of Tennessee-Murfreesboro/Nashville. Email: mark.reiter@yahoo.com.

EP Defendants Face Unpleasant Surprise: Med/Mal Policies Have Coverage Gaps

After emergency physicians (EPs) recover from the shock of finding themselves named in a lawsuit, jumpstarting a vigorous defense is probably top of mind. But what if the allegations are excluded by their professional liability coverage?

Medical malpractice policies are designed to cover exactly what their name suggests — liability arising out of medical professional services, says **Michael G. Merlo**, Esq., managing director of Casualty Legal and Claims Practice, Aon Broking. In reality, not many EPs carefully read their insurance policies.

"If the policy is provided by the employer, the EP might not even have ready access to it," Merlo notes. First, EPs need to understand what is excluded by their malpractice coverage. "Then, they should assess whether they have liability exposure in one of the excluded areas," Merlo says.

Here are some areas of risk that ED professional liability insurance typically doesn't cover:

• Emergency Medical Treatment and Labor (EMTALA) violations.

If an EP is accused of an EMTALA violation, the fine of up to $50,000 per occurrence is completely uncovered by insurance.

"You're on your own for that, and you may also be on your own for defense costs. In general, neither one is going to be covered," says **Andy Walker**, MD, FAAEM, an EP who provides legal consulting in defense of EPs.

Most Tennessee physicians are covered by physician-owned insurance companies, some of which do cover defense costs for alleged EMTALA violations. Several years ago, Walker was investigated for an alleged EMTALA violation. While his coverage wouldn't have covered any fines, it did cover his defense costs. Walker was ultimately exonerated.

How much would an EP pay out-of-pocket to defend against an alleged EMTALA violation?

"That depends on how long and contentious the investigation and prosecution are," says Walker. "It would have cost me about $4,000, and I never even had to talk to an investigator or judge — just my own lawyer."

While EMTALA regulations allow a hospital to be sued by a patient for an EMTALA violation, the individual EP cannot be sued. That doesn't necessarily stop a plaintiff attorney from filing suit against the EP, who then has to spend money to go to court just to have the suit thrown out.

"Even though courts in multiple jurisdictions have consistently ruled that EMTALA is not a federal malpractice statute, plaintiff attorneys will frequently threaten an EMTALA action," Walker says.

The alleged EMTALA violation is used as leverage to get the hospital — and sometimes the EP — to settle a malpractice claim.

"Even though those allegations are usually baseless, it still costs money to defend yourself," Walker says. "There is also the threat of a fine if the feds decide you are guilty."

• Allegations of criminal activity.

"In emergency medicine, this is not as farfetched as it sounds," Walker says, noting ED staff are sometimes the victims of physical attacks by patients or visitors. "That's just an unfortunate reality of our specialty. We all have the right to defend ourselves. You don't lose that right just because you are in a hospital."

If the local prosecutor decides that physical force used by the EP was not justified, the EP could end up charged with assault and battery. This is unlikely, however.

"I've never heard of a local prosecutor who came after an EP. Most are very sympathetic," Walker says.

The EP's response has to be proportional to the threat, Walker advises, and the EP should carefully document what happened.

Walker is unaware of any instances in which an EP was charged with criminal activity for something that happened while the EP was on duty in the ED, but says this has happened in other specialties. "There have been times where what should have been a civil suit was elevated to a criminal charge by the local DA when a patient died," he says.

Merlo says allegations of assault and battery are more likely against EPs than physicians in other specialties. This is because EPs have no prior relationship with their patients, who are sometimes under the influence of drugs or alcohol.

"Incidents in that environment are more likely, and could be expressly excluded, depending on the specific

policy wording," Merlo says.

• Intentional acts.

If the EP's conduct is truly intentional, not only the EP's actions, but also the injury the EP caused, "that's more likely to be excluded, even if it was otherwise a covered risk," Merlo says.

Policies typically have an "expected and intended" exclusion.

"If the EP intended to harm the patient, then there is less likely to be coverage, because it's more likely that would be considered an excluded intentional act under the law," Merlo says.

• Sexual harassment.

If a patient sues an EP for sexual harassment, or a local prosecutor alleges sexual assault, "those things are not covered, because they don't involve allegations of professional negligence," Walker says.

• Care provided outside the hospital the EP works in.

If the EP's coverage is provided by an emergency medicine group, "it almost certainly does not cover anything that you do medically outside of the hospital where you work," Walker says.

Similarly, if an EP receives coverage at one hospital, and also works at another hospital, the care provided by the EP at the second hospital is probably not covered unless that hospital provides the EP with a separate policy.

• Care provided informally.

Suppose an EP writes a prescription for amoxicillin for a neighbor's child, who has an allergic reaction, leading the parents to sue the EP.

"EPs need to remember when they're doing a favor for friend or neighbor, they are totally exposed," Walker says. "No matter how ridiculous or unfair the allegations might be, the EP has to pay for his or her own defense."

While most states have Good Samaritan laws to protect EPs legally, the EPs still have to go to court and defend themselves — at their own expense.

EPs often assume that their homeowners insurance or umbrella liability policy covers such situations.

"Almost all of them have a clause that excludes professional activity," Walker says. "Your malpractice insurance, which covers professional activity, doesn't apply outside the hospital."

A separate policy for such situations might be warranted.

"These policies may not be too expensive, because they exclude your primary workplace and just fill in the gaps. It's worth looking into," Walker advises.

• Defense against a complaint filed with the state licensing board.

Since this is not a civil lawsuit alleging professional negligence, the EP's defense is not covered by malpractice insurance.

"You can defend yourself, but that's a bad idea," Walker warns, noting the rules of evidence put the EP at a distinct disadvantage. "EPs do not have nearly the rights as a criminal defendant would. It costs money and is not covered, but you should retain counsel who is very experienced with state licensing issues." ■

SOURCES

- **Michael G. Merlo**, Esq., Managing Director, Casualty Legal and Claims Practice, Aon Broking, Chicago. Phone: (312) 381-5169. Email: mike.merlo@aon.com.
- **Andy Walker**, MD, FAAEM, Nashville, TN. Email: awalkermd@comcast.net.

Can Notes by Other ED Providers Force Settlement, or Help EP?

A recent malpractice case involved a patient who presented to an ED after a softball struck the patient in the head.

"Entries in the chart by various care providers made it difficult to pinpoint symptomology," says **Aaron Hamming**, JD, risk resource advisor, ProAssurance Companies.

One provider noted onset as sudden and acute, while another noted symptoms evolved gradually.

"In various other parts of the record, the patient was recorded upon arrival as not in acute distress, in pain distress, comfortable, and pain as nine out of 10," Hamming says. The patient was recorded as having abdominal pain and denying abdominal pain. "This, and other inconsistencies and contradictions, took a case that was initially viewed as extremely defensible and made it challenging," Hamming says.

Ultimately, the jury returned a verdict in favor of the EPs, whose care was almost unquestioningly appropriate.

"But it was a difficult defense because the record made it difficult to show that level of care," Hamming explains.

In another malpractice case, nursing notes described the patient's "headache and blurred vision," but the EP's template indicated "vision normal." The patient ended up with temporal arteritis and blindness in one eye. The lawsuit against the EP

settled for $200,000.

Nursing notes were also a key issue in a malpractice case alleging that the EP misdiagnosed a myocardial infarction as bronchitis. The triage nurse's note indicated "fever and chest pain."

"There was no documentation in the chart that the EP addressed the chest pain noted in the nurse's notes," says **John Davenport**, MD, JD, physician risk manager of a California-based HMO.

Conflict with documentation of other providers is a "common but avoidable area of ED risk," Davenport says. Here are two common examples:

• ED nursing notes that include abnormal vital signs that are not addressed in the chart;

• Nursing discharge notes describing a condition contrary to the EP's assessment.

"With the implementation of the EMR, and the use of templates or macros, these are becoming more common, and risk affecting the credibility of the physician," Davenport says.

Sloppy, Rushed Appearance

A skillful plaintiff attorney uses discrepancies in charting to argue that the EP failed to appreciate a crucial symptom or an important historical fact when evaluating or treating the patient, says **Judy Greenwood**, Esq., a Philadelphia-based medical malpractice attorney.

"This is particularly true where the nurse's note is more comprehensive," she says, noting the EP's failure to include pertinent findings is used to suggest the EP was sloppy or rushed in his or her approach. "A mismatch in the documented information can suggest a breach of care."

The defense of a malpractice case turns on a narrative: what occurred, how and when it happened, and why it all conformed with the standard of care, says **David S. Waxman**, JD, an attorney in the Chicago office of Arnstein & Lehr.

That defense can quickly unravel if inconsistent reporting of material elements undercuts the narrative.

"When a doctor and a nurse report on an event inconsistently, the physician's ability to tell her story, or set the narrative, is jeopardized, with potentially significant consequences," Waxman says.

A significant element of a narrative is the timing of events.

"Nothing is more damaging to a physician's story than to have a nurse chart that the physician was still present 15 minutes after the physician charted a shift change, or that an intubation was performed 7 minutes after a physician charted that it had been performed," Waxman says.

Inconsistencies on how much pain the patient is experiencing also come up frequently in malpractice litigation. The EP may chart that a patient is "stable with pain controlled," while the nurse records the patient's self-report of pain as 10 on a scale of 1 to 10.

"When that patient is later found to have an epidural hematoma with neurological sequelae, the doctor's defense has obviously been compromised," Waxman explains.

Acknowledge Other Views

Hamming says EPs need to think about the medical record "holistically."

"Too often — and EMRs are partly to blame — we see charts that are overly compartmentalized by section or responsibility," he says.

Inconsistencies in charting can be used to instigate ED providers into criticizing the care of other members of the care team.

"One way to combat this is to view the records as interrelated and interconnected," Hamming says.

EPs should be aware of what others are observing and documenting in the medical record.

"This does not mean that all providers must be in lockstep agreement about all aspects of the patient's care," Hamming says.

Rather, EPs should review and acknowledge other views and reports as part of their clinical evaluation, "as much as is reasonably practicable," Hamming says. "If a finding is different or inconsistent, it is OK to document that and include interpretation or discussion."

EPs might chart, for instance, that the patient's symptoms evolved, and that more studies or additional consultations are now needed.

"It can strengthen the defensibility of claims when the record shows a connection from a prior, inconsistent finding to the current one," Hamming says. ■

SOURCES

- **John Davenport**, MD, JD, Irvine, CA. Phone: (714) 615-4541. Email: Doctordpt@cox.net.
- **Judy Greenwood**, Esq., Law Offices of Judy Greenwood, P.C., Philadelphia. Phone: (215) 557-7500. Fax: (215) 557-7503. Email: greenwoodatty@aol.com.
- **Aaron Hamming**, JD, Risk Resource Advisor, ProAssurance Companies, Okemos, MI. Phone: (517) 347-6292. Fax: (517) 349-8977. Email: ahamming@proassurance.com.
- **David S. Waxman**, JD, Arnstein & Lehr, Chicago. Phone: (312) 876-7867. Email: DSWaxman@arnstein.com.

Will Plaintiff Attorney Sue EP, or Decide Claim Is Unwinnable?

ED chart can prevent — or inflame — litigation

A plaintiff attorney recently filed suit on behalf of a man who presented to an ED with a dog bite injury.

"It became infected and created some degree of chronic deformity of that finger. The attorney thought it looked like a good case," says **Michael Jay Bresler**, MD, a clinical professor of emergency medicine at Stanford University School of Medicine.

It soon became apparent the plaintiff attorney hadn't closely reviewed the ED chart, which stated the man had threatened to kill the EP and nurses. Documentation also indicated the man refused to allow them to clean the wound.

"He was given a prescription for antibiotics, which was never filled. It wasn't until 6 weeks later that he saw a doctor," Bresler says. "It was clear from the record that there was no case."

The attorney sent the EP a notice of intent to sue, and the EP threatened to countersue for malicious prosecution.

"The case never went anywhere," Bresler says.

Misleading charting caused a plaintiff attorney to name an EP in a lawsuit involving intubation of a post-operative patient. In this case, the EP was called to the ICU to intubate a postop patient.

"The EP couldn't get the ET tube in, and finally called the anesthesiologist," says Bresler, who was an expert witness in the litigation.

The EP's note simply stated, "Couldn't get the patient intubated." The anesthesiologist charted, "Multiple attempts by EP, tube was in the esophagus, patient re-intubated."

"The patient ended up with brain damage," Bresler says. "From the chart, it appeared the EP had messed up the intubation."

In subsequent depositions, both the nurse and respiratory therapist stated that the EP had ventilated the patient adequately between attempts. The anesthesiologist was able to get the tube in, but the patient had become hypoxic when the anesthesiologist decided to readjust the tube. Their testimony made it clear that the anesthesiologist was the one who intubated the esophagus.

The plaintiff attorney told Bresler that he never would have named the EP in the lawsuit if the EP's documentation had been better.

"The anesthesiologist's misleading documentation — and the EP's cursory documentation — skewed what really happened," he explains. "After years of litigation, it turned out that the wrong doctor was sued."

Most Cases Rejected

Ideally, the ED chart, on its own, will convince any plaintiff attorney or hired expert that the standard of care was met.

"We want it to say everything that we want them to know, without even going to a deposition stage, that it would be a waste of time to pursue the lawsuit," Bresler says.

The plaintiff attorney must decide if it's worth paying an expert to review the ED chart.

"If it's not winnable or it's marginal, many will just not take the case," Bresler says. "The plaintiff attorneys that I know and respect say they reject about 90% of cases that are brought to them."

A record showing referral to a specialist or appropriate tests ordered, with a clear sequence of events and sufficient detail, makes it harder for a plaintiff attorney to bring a case, says **Jonathan D. Rubin**, JD, an attorney at Kaufman Borgeest & Ryan in New York.

"When it's not clear about what happened with who and when, it's problematic," Rubin says, noting that because plaintiff attorneys work backward, they know a result and look at it in hindsight. "If there are gaps in the chart, they can fill those in with their suppositions and 'could have beens' and 'should have beens.'"

Some cases seem appealing initially, but fall apart under scrutiny. A common example: family members who insist tissue plasminogen activator should have been given to their loved one who suffered a bad outcome after a stroke.

"The attorney may think they have a really good case, but after reviewing the chart, they realize the determination of onset of symptoms was pretty vague," Rubin says.

Since the odds of plaintiff's attorney winning a given case are relatively low to begin with, they tend to be selective about which cases they will take, says **Marc E. Levsky**, MD, vice chair of the board of directors, The Mutual Risk Retention Group. "This is especially true when they are being paid on a contingency — a percentage of any monetary award to the plaintiff," he notes. Here are some factors plaintiff attorneys consider:

• Whether there was negligence and causation.

"If there is no negligence, or the causation of damages by the alleged negligence is very questionable, the plaintiff's attorney would be much less likely to take the case, as their chance of success is greatly diminished," Levsky says.

A family recently threatened to sue an EP because the patient, an 86-year-old man, had allegedly suffered worsening of his condition and death due to ED care.

"The patient, who was being seen in the ED for abdominal pain and suspected sepsis, did indeed have worsening of his CHF [congestive heart failure] after he was treated with IV fluids in the ED," Levsky says.

The chart indicated that the family told the EP about the fact that the patient was "very fluid-sensitive and tends to go into CHF" only after the fluid had already been given. The treatment the EP provided clearly met the standard of care — for abdominal pain in the elderly, sepsis, and CHF.

"Finally, the patient had a history of end-stage lymphoma, which itself carried a very poor prognosis," Levsky explains. "Given that his death came two months after the episode of ED care in question, causation was lacking."

When the EP received the complaint and 90-day notice of intent to file suit, it notably came from the patient's daughter and not from an attorney.

"We surmise that the patient's family could not find an attorney who was willing to take the case. The lawsuit was never filed," Levsky adds.

• The potential for damages.

"Plaintiff attorneys are more likely to gamble on a weak case if the potential award for damages is large," Levsky says.

For example, attorneys likely would reject a claim involving the death of a very elderly person who suffered from multiple medical problems, without even reviewing the records.

"Damages would likely be small, and causation would be hard to prove," Levsky explains.

• Whether there was contributory negligence on the part of the patient or family.

Did the patient fail to adhere to the EP's documented recommendations?

"This would make the case harder to win," Levsky says.

• Whether there was questionable plaintiff behavior.

Even a strong malpractice case gets complicated if the patient used inappropriate language, was violent in the ED, or had a history of substance abuse or criminal acts.

"A jury would probably be less sympathetic toward a plaintiff who is alleging that he was injured by a physician who was trying to treat his injuries, which he sustained while being arrested for robbing a liquor store," Levsky says.

The defense attorney would have little trouble questioning the credibility of this plaintiff. Documentation showing the EP spent a great deal of time with the patient, and that the patient was satisfied with the care, also makes the case less appealing.

"If the attorney gets the sense that the jury would be more sympathetic to the physician than the patient, they would be less likely to take the case," Levsky says.

• Whether the plaintiff is being truthful.

One patient sued an EP, alleging that he was rendered completely disabled and nearly paralyzed due to ED care.

"During the trial, he was shown on video swimming long distances in the ocean and playing golf," Levsky notes.

In another case, a deceased patient's wife stated in a deposition that her husband had never been denied life insurance. In the patient's medical records, there was a signed note from her to the patient's primary physician requesting help because the patient had been denied life insurance.

"The plaintiff's attorneys in both of these cases lost a significant investment of resources," Levsky says. ■

SOURCES

- **Michael Jay Bresler**, MD, Clinical Professor of Emergency Medicine, Stanford University School of Medicine. Email: bruzl@aol.com.
- **Marc E. Levsky**, MD, The Mutual Risk Retention Group, Walnut Creek, CA. Phone: (925) 949-0100. Fax: (925) 262-1763. Email: levskym@tmrrg.com.
- **Jonathan D. Rubin**, JD, Kaufman Borgeest & Ryan, New York. Phone: (212) 994-6515. Fax: (212) 980-9291. Email: jrubin@kbrlaw.com.

WE NEED YOUR HELP!

The editors of *ED Legal Letter* are planning more topics and articles for 2016 and would like your feedback. Please help us by answering three questions at the following link:

https://www.surveymonkey.com/r/ELBSurvey2016

Thank you for your time and input!

ED LEGAL LETTER™

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. Scan the QR code to the right, or log onto **AHCMedia.com** and click on My Account. First-time users will have to register on the site using the 8-digit 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 to achieve a score of 100%.

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 directed to an activity evaluation form, which must be completed to receive your credit letter.

CME/CE QUESTIONS

1. **Which of the following statements is true regarding hospital liability involving cyberattacks?**

   A. If the hackers sold patient information, the hospital would be subject to claims for damages for identity theft from its patients.
   B. If the hospital has confirmed that patient care was not compromised and no personal information of the patients was stolen, the hospital likely does not face much liability.
   C. If patient care was compromised, the hospital could potentially face claims of professional negligence.
   D. All of the above statements are true.

2. **Which is recommended to avoid EMTALA violations?**

   A. Co-pays over $100 should not be collected upfront.
   B. The medical screening exam and any medical care needed to stabilize an emergent medical condition should never be delayed as a result of obtaining any financial information — including collecting co-pays.
   C. The hospital has no right to insist on payment for non-emergent care provided in the ED.
   D. Hospitals can request co-pays before stabilization treatment in some cases.

3. **Professional liability insurance policies typically cover:**

   A. liability arising out of medical professional services.
   B. defense against EMTALA violations, including payment of fines.
   C. sexual harassment alleged by patients.
   D. care provided outside the hospital.

4. **Which of the following statements is true regarding plaintiff attorneys' decision on whether to pursue an ED claim?**

   A. Attorneys pursue the majority of cases brought to them.
   B. Onset of symptoms is irrelevant in cases alleging failure to administer tissue plasminogen activator (tPA) to stroke patients.
   C. Plaintiff attorneys are more likely to pursue a weak case if the potential award for damages is large.
   D. Any attorney need not consider the patient's contributory negligence in weighing the merits of a case, since any negligence by the ED physician is actionable.