HEALTHCARE RISK MANAGEMENT™

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

INSIDE

RELIAS MEDIA

DECEMBER 2018 Vol. 40, No. 12; p. 133-144

Cyberinsurance Now a Necessity, But Choose Coverage Wisely

Insurance to cover cyberattacks leading to data breaches, ransom, and interference with medical care is becoming more popular with hospitals and health systems, almost becoming as much a necessity as malpractice coverage and general liability insurance. Choosing the right coverage requires understanding the available options and the needs within your own organization.

The risk of a data breach and the potentially huge costs were highlighted in the recent $115 million settlement resolving a 2015 data breach at insurer Anthem. The breach exposed the records of 78 million members. *(For more information on the settlement, see the story on page 139.)*

> CYBERINSURANCE CAN HELP MINIMIZE THE RISKS ARISING FROM HACKERS AND OTHER VULNERABILITIES, BUT IT IS ONLY ONE PART OF AN OVERALL CYBERRISK PROGRAM.

Cyberinsurance can help minimize the risks arising from hackers and other vulnerabilities, but it is only one part of an overall cyberrisk program, says **Kenneth K. Dort**, JD, partner with the law firm of Drinker Biddle in Chicago. The type and extent of cyberinsurance an organization should buy depends on the types of data stored and processed by that company, as well as the amount of resources that the company can afford to devote to cyberdefense in general, he says.

The hospital or health system considering cyberinsurance needs to identify its specific vulnerabilities and threat profiles to ascertain what contingencies it wants to protect against, Dort says.

ReliasMedia.com

Financial Disclosure: Author **Greg Freeman**, Editor **Jill Drachenberg**, Editor **Jesse Saffron**, Editorial Group Manager **Terrey L. Hatcher** and Nurse Planner **Maureen Archambault** report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study. Consulting Editor **Arnold Mackles**, MD, MBA, LHRM, discloses that he is an author and advisory board member for The Sullivan Group and that he is owner, stockholder, presenter, author, and consultant for Innovative Healthcare Compliance Group.

HEALTHCARE RISK MANAGEMENT™

Healthcare Risk Management™, ISSN 1081-6534, including Legal Review & Commentary,™ is published monthly by Relias Learning, 111 Corning Road, Suite 250, Cary, NC 27518-9238. Periodicals postage paid at Cary, NC, and additional mailing offices. POSTMASTER: Send address changes to Healthcare Risk Management, Relias Learning, 111 Corning Road, Suite 250, Cary, NC 27518-9238.
GST Registration Number: R128870672

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

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

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

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

Relias LLC is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians.

Relias LLC designates this enduring material for a maximum of 1.5 *AMA PRA Category 1 Credits™*. Physicians should claim only credit commensurate with the extent of their participation in an activity.

Healthcare Risk Management™ is intended for risk managers, healthcare administrators, healthcare legal counsel, and physicians.

This activity is valid 36 months from the date of publication.

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

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

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

"This comes from a detailed exchange with its insurance broker who can then provide the company with multiple insurance options, packages, and pricing from which to select and which best meet its risk considerations and pricing needs," Dort says.

There are many options covering the entire spectrum of risks and system protections, Dort notes. It is important to understand what any specific proposed package covers, he says.

Many packages also include access to relevant cyberexperts through the insurance company's preferred panels, such as forensic investigators, attorneys, and credit-monitoring services. Those resources can be valuable, but if you are considering one of these packages you should confirm whether you still can use experts of your own choosing within such coverage, Dort says.

Variety of Options Available

Policies can vary widely from insurer to insurer, notes **Steve Durbin**, managing director at Information Security Forum (ISF), a nonprofit organization based in London. He says there are two primary areas of coverage to be familiar with: cyberliability insurance and cyberrisk insurance.

Cyberliability insurance provides cover for liabilities that an organization causes to its customers or to others, he explains.

"A sizeable market exists for these products. It can cover data breach and crisis management, including incident management, investigation, data subject notification, credit monitoring, legal losses, and so on, plus media liability for something like website defacement, extortion liability, and network security liability," he says.

Cyberrisk insurance is used to cover direct losses to the organization. It is less common not only because insurers still lack meaningful data, but also because many organizations assume that their corporate or general liability policies will cover cyberrisk, Durbin says.

That may not be the case, Durbin says. Always check before assuming you are covered.

"Cyberrisk insurance may include some liability coverage, but it can more broadly cover liability, copyright, effects of malicious code, business interruption, cyberattack, technology errors, and omissions and intellectual property infringement," he says. "The market continues to develop, and using insurance products to treat cyberrisk is an option for many organizations. It is important to note, however, that although insurance will transfer

EXECUTIVE SUMMARY

Cyberinsurance is becoming a necessity for healthcare organizations. Coverage should include data breaches originating both inside and outside of the hospital or health system, as well as ransomware and malware.

- Understand the exclusions of a cyberinsurance policy.
- The number of files protected will influence the cost of coverage.
- Insurers will carefully assess your cybersecurity program.

a precise amount of risk to the insurer, there will be cyberrisks that cannot be transferred and which an organization will have to deal with outside of any insurance policy."

Now a Necessity

Cyberinsurance is necessary in the eyes of **Avery Dial**, JD, partner with the law firm of Kaufman Dolowich & Voluck in Fort Lauderdale, FL.

"In this era, you definitely need cyberinsurance," Dial says. "Furthermore, data theft and loss are not the only concerns. Data-destroying malware and ransomware is also a major concern."

These threats give rise to first- and third-party risks, Dial explains. For instance, a hospital may make a first-party claim when it must pay for restoration of data destroyed by malware. That same event may also cause harm to third parties who may sue the hospital for damages caused by the destruction of the data, he says.

"Cyberpolicies may cover both first- and third-party risks specific to cyberthreats. While many people have tried to stitch together coverage for cyberevents via commercial general liability policies or property insurance policies, businesses should not rely on traditional insurance policies to cover cyberevents," Dial says. "The cost is worthwhile because it is necessary. It is almost inevitable that you, as a business, will experience a cyberevent — and the consequences can be quite costly."

Like all insurance, your premium will be determined by your risk profile, Dial notes. There is no one insurance product that will fit all healthcare organizations, he says. With the help of an IT professional, the hospital should identify the particular risks to which it is most susceptible and insure against those risks, he says.

Healthcare organizations will be presented with multiple coverage options — coverage for breach notification, data restoration, extortion, and business interruption, and third-party coverage for data breach and privacy liability. Policies also may cover regulatory and government investigations and coverage for fines assessed by credit card companies in the event of a breach, Dial explains.

Threats Are Growing

Cyberinsurance is increasingly important in the healthcare industry, says **Michael Tanenbaum**, executive vice president of North America Cyber Practice at Chubb Limited, which provides cyberinsurance for healthcare organizations of all sizes. Healthcare organizations represent nearly one-third of all cyberinsurance claims for Chubb in the past three years, he says.

The company's Cyber Index tracks cyberinsurance claims since 2009. Tanenbaum says the trend is clear that healthcare organizations are among the most vulnerable to this type of loss. *(The index is available online at: https://bit.ly/2KDKoyE.)*

"Healthcare in general is represented in 31% of our cyberclaims in the past three years, and over the entire inventory of cyberclaims it represents 25% of our claims. That is 10 points higher than the next leading industry," Tanenbaum says. "That is disproportionate to the amount of healthcare risk we write."

Healthcare organizations may primarily think of cyberinsurance for covering the most obvious costs related to an accidental data breach, including notification, forensics, and crisis management, Tanenbaum says, but there can be substantial other expenses. Ransomware and destructive malware are growing threats, he adds.

Attacks in recent years have crippled healthcare organizations' data systems, notably the May 2017 Wannacry attack that used a ransomware cryptoworm to target computers running Microsoft Windows, encrypting data and demanding ransom payments in the cryptocurrency Bitcoin. The British National Health Service was affected so much that patient care was compromised.

Another encrypting ransomware, NotPetya, attacked healthcare organizations in 2017.

"A medical transcription company was greatly impacted by NotPetya, and as a result a lot of hospitals could not perform surgery or do a lot of other healthcare operations because they had no transcription service. For that company hit by the ransomware it was a revenue loss, but the effects of that attack spread beyond that company to affect hospitals and other organizations," Tanenbaum explains.

The transcription company announced that its transcription software was taken offline by the attack. Ten other products were affected as well, including those used for radiology, billing, and tracking quality of care.

Insurers have followed the expansion of cyberthreats by offering more types of coverage, Tanenbaum says. These may include incident response, risk transfer, and pre-breach security improvements.

Risk managers must find the

right mix of coverage, addressing the risk of outside attacks like Wannacry and NotPetya while also covering the more mundane but very real exposures within their own organizations, Tanenbaum says.

"Our index of claims shows that the number-one issue for healthcare is internal employees, poor controls, lost and stolen laptops, and human error," he says.

"Risk managers can be more diligent about training employees in things like how to handle paper files, phishing attacks, and what it means to click on links. Phishing represents roughly 40% of all the breaches we've handled."

The need for cybersecurity and cyberinsurance has much to do with the value of protected health information (PHI) on the dark web, notes **Roy Hadley, Jr.**, JD, special counsel with the law firm of Adams and Reese in Atlanta, and a former chief privacy officer. Credit card information used to be most sought by criminals seeking to use data fraudulently, but that has now been eclipsed by healthcare information, he notes.

Stolen PHI can contain far more data on a single person than just a credit card, making it more useful for stealing a person's identity or committing other fraud, he notes. Credit cards also can be canceled quickly once the data breach is discovered, but healthcare PHI remains usable. That is why healthcare PHI trades for a much higher price on the dark web than credit cards or similar financial information, he says.

"The damage that can be done to an individual financially can be catastrophic. Because of the type of information any healthcare organization collects on its patients, the risk faced from losing control of that information is going to be high," Hadley says. "I tell all clients to look at your risk profile and make cyberinsurance a part of your program if necessary, but for healthcare organizations the risk profile almost necessitates cyberinsurance for all of them."

Hadley also advises healthcare clients to take advantage of the cyberinsurance application process to improve their cybersecurity. Underwriters for cyberinsurance will take a close look at how the organization addresses cybersecurity and price premiums accordingly,

Watch for Common Pitfalls in Cybercoverage

Healthcare risk managers may mistakenly assume that a commercial insurance policy will cover the damage related from cyberattacks, but that is often not the case, says **Chris Frederick,** partner with the tax and accounting firm Bennett Thrasher in Atlanta.

Even if the policy is written in such a way that it could cover cyberdamages, it is common for policies to require evidence of physical damage before any coverage kicks in — and there usually is none in a cyberattack, he says.

Healthcare organizations also may run into trouble with the cyberinsurance provider determining that the cyberattack occurred due to insufficient security.

"The insurance company will look at whether the network infrastructure was secure enough. They might say basically, 'Yes, there was a data breach, but you didn't take the necessary steps to prevent it,'" Frederick says.

Frederick also has worked with a company that experienced a data breach and found that the insurer did not want to cover satellite locations, including employee homes, because those locations were not named in the policy.

The limits on coverage also are important. For instance, if a policy covers the IT work necessary to recover from an attack, does that mean the insurer will reimburse you for the time your own IT employees spend on it? Or only for outside IT consultants, because your employees would have been paid for their work anyway? Frederick has seen companies surprised and frustrated when the insurer refused to compensate them for the work performed in-house.

"A key component is to know exactly what is covered and what is not," Frederick says. "Even if it doesn't cover all that you wish it did, possibly because you can't afford that level of coverage, you are better off knowing that up front and not after you have been attacked." ■

SOURCE

- Chris Frederick, Partner, Bennett Thrasher, Atlanta. Phone: (678) 218-1403. Email: chris.frederick@btcpa.net.

so going through that process can reveal opportunities for improvement, he says.

"Whether you get their insurance or not, you can see the holes in your program and then work on minimizing any issues that are found and patching the holes that they find," he says.

The best way to begin seeking cyberinsurance is to work through the broker already providing other types of insurance for the healthcare organization, Hadley says. This person already will be familiar with the organization and should be able to access products from many insurers. Many of the options will be familiar from the organization's other insurance coverage, such as retention or self-insurance figures.

The size of the organization will be a critical factor in determining the amount of coverage, Hadley explains, because many of the costs associated with a data breach are determined per patient or per record.

"If you are holding a million patient files in your portfolio, a big hospital system, then $1 million in cybercoverage isn't going to help you. If you have a data breach, the cost of notification, credit monitoring, and other expenses can easily get to be $50 to $100 per patient. When you start multiplying that out, $1 million isn't going to go very far," Hadley says. "You also have to consider your risk exposure from, for instance, transferring files back and forth across different systems as opposed to being one standalone hospital that doesn't carry as much of that risk."

Watch the Exclusions

When selecting an insurer, inquire about the company's payment history, Hadley advises. Cyberinsurance is still a relatively new product in the insurance industry, so hospitals should ask to see evidence that the insurer has a history of paying legitimate claims, he says. A lack of paid claims may indicate that the policies are written so as to deny many claims or that the insurer simply does not have enough experience in the field, he says. *(For more on selecting an insurer, see the story on page 138.)*

Also be wary of the boilerplate exclusion for acts of war or terrorism, Hadley says.

"If it is a nation-state actor like North Korea that is trying to access your hospital system, is that an act of terrorism or an act of war? Depending on how your policy is worded, that policy might not be applicable to your incident," he says. "That becomes important when we see these countries involved in widespread cyberattacks."

Policies also might specify that they will pay only for unauthorized access to data. That may sound reasonable since a breach is generally some type of unauthorized access, but such a provision could be problematic, Hadley says.

"The problem is that a rogue employee may cause a data breach that caused you harm, and some insurance companies will say that employee has authorized access so you are not covered," Hadley says. "The exclusions and riders on the policy must not be so broadly written that they can exclude what would probably happen to you in a cyberincident — the whole reason you're getting the insurance." ■

SOURCES

- **Avery Dial**, JD, Partner, Kaufman Dolowich & Voluck, Fort Lauderdale, FL. Phone: (954) 712-7442. Email: adial@kdvlaw.com.
- **Kenneth K. Dort**, JD, Partner, Drinker Biddle, Chicago. Phone: (312) 569-1458. Email: kenneth.dort@dbr.com.
- **Steve Durbin**, Managing Director, Information Security Forum, London. Email: steve.durbin@securityforum.org.
- **Roy Hadley Jr.**, JD, Special Counsel, Adams and Reese, Atlanta. Phone: (470) 427-3730. Email: roy.hadley@arlaw.com.
- **Michael Tanenbaum**, Executive Vice President of North America Cyber Practice, Chubb Limited, Warren Township, NJ. Phone: (866) 324-8222.

Expanding Cyberinsurance Market Brings Benefits to Healthcare

The expansion of the cyberinsurance market means that healthcare organizations can get more coverage for a lower premium than in the past, notes **Alex Purvis**, JD, partner with the Bradley Arant Boult Cummings law firm in Jackson, MS. Insurers also are building experience in paying claims, which helps them write policies that are realistic in terms of what they cover and what is excluded, he says.

Insurers focusing on cyberinsurance will have the best grasp and be able to pay legitimate claims, he says.

"The insurance policies that are cyberspecific tend to respond to the claims. The cyberinsurance industry tends to be a little more claim-friendly than you might see in some other insurance arenas," Purvis says. "That's another advantage to the market being so competitive now. These insurers don't want to get the reputation that they accept your premium dollars, but when you submit a claim they refuse to pay it based on some tiny language on page 12 of their insurance policy."

Some commercial general liability (CGL) insurance policies will cover the losses associated with a data breach, but that is becoming less common now that insurers recognize the size of that risk and prefer covering it with specific cyberinsurance policies, Purvis says. More CGL policies now specifically exclude the cyberrisk, making it more important to purchase a cyberpolicy, he says.

Purvis also cautions risk managers about the importance of putting the insurer on notice once a data breach or other covered cyberincident is discovered.

"What keeps me up at night as a policyholder lawyer is the fear that I've got a bunch of clients who are facing a claim but have not put their carriers on notice," Purvis says. "They may have a great insurance product, but if they don't put them on notice they may lose the opportunity get the coverage they've already paid for."

Consult IT Team

Healthcare organizations are adopting cyberinsurance more readily than in the past, says **Benjamin P. Malerba**, JD, partner with the Rivkin Radler law firm in Uniondale, NY. Policy limits for a hospital or other healthcare organization typically are between $3 million and $10 million, he says.

"You want to be sure that the coverage is not only going to provide you with defense against the cyberattack, but that it also will cover your costs related to a data breach, the notifications of not just the patients affected but also the government. In many cases, you will have to notify different branches of the federal government, law enforcement, and — since so much healthcare is delivered across state lines — multiple state governments," Malerba says. "Those costs can really add up. Even just the postage can add up if you have a large data breach, and there can be additional costs like writing the notification in several languages."

To obtain cyberinsurance, a healthcare organization's risk manager or compliance officer should first meet with an IT professional to determine the scope of the data and risk, and the security of the IT systems, says **Ananth Avva**, CFO at enterprise network security provider Lastline in Redwood City, CA. Consider factors such as whether you operate only in the United States, or internationally.

"Cyberinsurance insurers are also very good at customizing a policy to the needs of your institution. They can slice and dice the different options to tailor it for your needs, giving you a package that is commensurate with your level of risk," Avva says. "But for that to happen, you first have to have a good understanding of where your particular organization stands on these different factors that comprise your cyberrisk profile."

The most common error Avva sees when procuring cyberinsurance is having the CFO or compliance office drive the conversation with the insurer, when that person is not the one most familiar with the organization's data and risks. The IT department should be heavily involved in the purchasing effort, if not driving it, Avva says.

"If those two groups don't communicate and the CFO buys cyberinsurance just to check off a box somewhere, that's where you're going to see pretty big gaps," Avva says. "Cyberinsurance is not all the same, and you may discover later that the CFO or compliance officer didn't really understand what was covered and what was not. They don't understand it the same way the IT team does."

It is useful to think of cyberinsurance as filling in gaps in existing insurance coverage, says **Andrew Gibbs**, partner at the law

firm of Lindabury, McCormick, Estabrook & Cooper in Westfield, NJ. While filling those gaps, a healthcare organization should strive to have overlapping coverage.

For example, an existing policy may already cover social engineering, the type of attack that uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

"Cyberinsurance can fill in gaps, and in some cases give you interlocking or overlapping coverage," Gibbs explains. "A large organization might have a crime policy with a social engineering endorsement, and then if you get a standalone cyberpolicy that also has social engineering coverage, you'll have an overlap. That overlap helps protect you because those policies are going to limits and exclusions that might be overcome by the other policy."

Cyberinsurance tends not to be expensive compared to other coverage, Gibbs says, but be careful to understand exactly what the policy provides. Deductibles should be considered carefully.

"There may be higher deductibles for certain kinds of cyberlosses, so healthcare organizations should get with their brokers or lawyers and try to maximize the coverage they can get within their financial restraints," Gibbs says. "They also should watch carefully for exclusions and language that lessens the coverage." ■

SOURCES

- **Ananth Avva**, CFO, Lastline, Redwood City, CA. Phone: (877) 671-3239. Email: aavva@lastline.com.
- **Andrew Gibbs**, Partner, Lindabury, McCormick, Estabrook & Cooper, Westfield, NJ. Phone: (908) 233-6800. Email: agibbs@lindabury.com.
- **Alex Purvis**, JD, Partner, Bradley Arant Boult Cummings, Jackson, MS. Phone: (601) 592-9923. Email: apurvis@bradley.com.
- **Benjamin P. Malerba**, JD, Partner, Rivkin Radler, Uniondale, NY. Phone: (516) 357-3128. Email: benjamin.malerba@rivkin.com.

Anthem Settlement Holds Lessons on Data Breaches, Costs

Anthem's recent $115 million settlement — one of the largest ever in a consumer data breach — shows how costly a breach can be for a healthcare organization. Risk managers should remember that even a much smaller breach could be financially devastating.

A California federal district judge approved the settlement resolving a 2015 data breach at Anthem that exposed the data of 78 million members. The settlement will be divided among 19.1 million plaintiffs in the class-action lawsuit. Each can claim up to $10,000 to cover out-of-pocket expenses related to the breach and can receive free credit monitoring services beyond what Anthem has already provided. *(The settlement agreement is available online at: https://bit.ly/2jx3ehy.)*

While the numbers and costs associated with this breach are staggering, the issues at the root of it are quite simple, says **Dianne J. Bourque**, JD, an attorney with the Mintz law firm in Boston.

"Someone clicked on a phishing email, intruders gained access to Anthem's PHI [protected health information], and the ensuing enforcement action revealed that Anthem has no enterprisewide risk analysis," Bourque says. "We see this fact pattern almost daily. The only thing different about the Anthem case is the large number of individuals affected."

"The Anthem breach should stand as a reminder to healthcare risk managers that this could easily happen to their organizations if they don't pay attention to compliance fundamentals, especially a comprehensive security risk analysis, ongoing employee training — both formal and informal — and information system activity review," she added.

The Anthem breach should strike fear in healthcare leaders, says **Mark Bower**, general manager and chief revenue officer with Egress Software in Boston.

"This is a shot across the bow for every CEO, CIO, and CFO," Bower says. "Not every organization can absorb settlements of this size, not to mention the ongoing management and escalation costs, punitive fines from regulations like HIPAA and GDPR [General Data Protection Regulation], and revenue losses from customer churn that are also associated with data breaches."

The class-action suit shows that consumers possess a healthy appetite for compensation following a breach of their data, Bower says. Organizations that handle PHI, especially highly sensitive patient data, should use this to gauge what is acceptable financial risk when securing data, and invest in

technology and training accordingly, he says.

A Single Click Causes Chaos

"There's no compromise when it comes to data security. Organizations must always be on the front foot when protecting sensitive data, ensuring their policies and technologies are up-to-date and can mitigate emerging risks," Bower says. "This attack stemmed from a single phishing email that one unsuspecting employee opened, enabling a hacker to gain access to nearly 79 million data records. The scale of this is incredible, and even the smallest perceived risk must be dealt with."

Often, people are the point of weakness, Bower says. Recent years have brought radical changes in the way employees work and consume IT services, including the rise of mobile and remote working, and cloud computing.

"Users have become the new security perimeter, and the surface area for risk has increased exponentially as a result. Organizations now need to do more to put guiderails in place to enable employees to work both efficiently and securely," Bower says. "Phishing emails must be intercepted whenever possible and the best security put in place to mitigate a breach if they do end up clicking on a malicious link."

Risk managers need to honestly evaluate whether their organizations can afford to be the next Anthem, Bower says.

"Almost every employee will be sent a phishing email at some point or other, and organizations need to ensure their data is protected against this risk. Poor security and a failure to protect patient data carries real, financial consequences that impact the company and shareholders," he says. "Cybersecurity must have a place at the table in the broader discussion of risk tolerance."

Logging and log monitoring were highlighted in this case, notes **Doug Kanney**, principal and the practice lead for HITRUST and HIPAA with Schellman & Company, an independent IT audit and certification firm in Tampa, FL.

"The investigations found that the monitoring of key logs was not taking place that would have helped identify the malicious activity much sooner. Strong password controls were also not found to be in place to adequately protect this highly valuable ePHI," Kanney explains.

"It was noted in the OCR [Office for Civil Rights] Resolution Agreement with Anthem that strong password controls should be put in place, and it specifically calls out password age," he continues. "The risk analysis was not enterprisewide, which I believe played a large part in the enforcement action size. A risk analysis was performed, but it was too narrow and did not account for all locations ePHI was residing."

For risk managers, Kanney says these enforcement actions highlight what OCR has consistently tried to demonstrate during its past enforcement actions: The risk analysis/risk management process is the cornerstone of a sufficient HIPAA compliance program.

More than 90% of HIPAA enforcement actions to date by OCR have pointed to an insufficient risk analysis/risk management program, so this is not new, Kanney says.

"The flow of ePHI in your environment should be mapped to ensure that all systems that may contain ePHI are considered as part of the risk analysis. If it is unclear what systems might contain ePHI, all systems should be considered in scope for risk analysis and security controls," he says.

"It is important to have a process to perform a risk analysis on a recurring basis, typically at least annually. A process also should be in place to perform ongoing risk analysis if major changes occur in business or if new types of technology are introduced that have a significant impact on the environment." ■

SOURCES

- **Dianne J. Bourque**, JD, Mintz, Boston. Phone: (617) 348-1614. Email: dbourque@mintz.com.
- **Mark Bower**, General Manager and Chief Revenue Officer, Egress Software in Boston. Phone: (800) 732-0746.
- **Doug Kanney**, Principal and Practice Lead for HITRUST and HIPAA, Schellman & Company, Tampa, FL. Phone: (866) 254-0000.

EXECUTIVE SUMMARY

Anthem has settled a data breach case for $115 million. It is one of the largest settlements ever and holds lessons for healthcare risk managers.

- The breach was traced to one employee clicking on a link.
- Investigators cited insufficient monitoring of key logs.
- The case illustrates the importance of a robust risk analysis/risk management program.

Nursing Shortage, Technology Changes Could Bring Liability Risks

The new year will bring nursing-related liability risks that involve the aging labor force, the changing healthcare industry, and technology, says an industry analyst. Risk managers should anticipate these issues and be ready to respond to new risks.

The aging labor force in nursing will create more potential liability for healthcare organizations, says **David Griffiths**, senior vice president for program management with consulting firm Aon in Fort Washington, PA. About a half-million nurses will retire over the next two years, he says, at the same time the industry has an increased need for nurses with expanded skill sets.

Sicker Patients for Fewer Nurses

"There is the added demand and we just don't have enough nurses coming in. We're looking at a labor shortage in the next couple of years," he says. "You add the expanded roles of nurses to that, the way we're asking more of nurses now, and the problem only gets worse. A shortage of skilled nurses can only increase the potential liability for healthcare organizations that will have to find a way to care for patients despite the shortage."

Increasing healthcare costs and continuing difficulty with the insurance market are making patients put off healthcare, Griffiths says, and that means their conditions are more acute when they do seek treatment.

"Nurses will be faced with more acute cases at the same time they are in short supply," he says. "Fewer nurses will be taking care of sicker patients. That is not a recipe for success."

New Pathways for Care

The mergers of big companies like CVS and Anthem to create new pathways for delivering healthcare will bring uncertainty into many facets of the industry, putting nurses in new care settings with unknown potential for liability, Griffiths says.

"Those mergers and new companies will change the dynamic of how healthcare is managed, with nurses in those new settings that are not physician offices and not hospitals, with new exposures and risks surrounding that," he says. "It's going to be an interesting world for nurses in the future, and an interesting world often brings the potential for new risks and exposures."

Technology also will continue to change the role of nursing, with machine learning and artificial intelligence helping to improve nurse diagnosing, Griffiths says.

"I think we're going to see more of that in small waves in 2019. The implications for risk management is really unknown because the impact on nurse diagnosing is unknown," he says.

"We have seen some examples in which artificial intelligence was a great aid to nurse diagnosing in an emergency setting, but we have not had enough experience with the technology to know the potential for good or bad."

Griffiths advises risk managers to proceed cautiously when artificial intelligence is introduced to a clinical setting.

"Introducing artificial intelligence to the diagnosis of patients, from a risk management standpoint, has incredible upside opportunities. But I would roll that out in a very closely monitored scenario rather than just plug and play," he says.

"Any technology that helps reduce the administrative burden, however, could work to reduce risk and exposure because you could then leverage the resources and capabilities of the nurse to a more efficient use." ■

EXECUTIVE SUMMARY

Hospitals and health systems are likely to face a nursing shortage in the next two years. This could increase potential risk and liability.

- Clinicians will be treating more acute patients who have put off healthcare services for financial reasons.
- New pathways for delivering care could introduce new risks.
- Artificial intelligence will make more inroads into healthcare but should be adopted cautiously.

SOURCE

- **David Griffiths**, Senior Vice President for Program Management, Aon, Fort Washington, PA. Email: david.griffiths@aon.com.

Sexual Harassment Is a Serious Issue in Healthcare Settings

Sexual harassment occurs more frequently in healthcare settings than risk managers might imagine, and the potential liability can be significant, says **Jennifer Flynn**, CPHRM, manager in the healthcare risk management division of consulting firm Aon in Fort Washington, PA.

She points to a 2016 report on sexual harassment claims from the Equal Employment Opportunity Commission that found that from 2005 to 2015, 11% of claims were from the healthcare and social assistance industry. *(The report is available at: https://bit.ly/29nQYXI.)*

"That was the fourth-highest in comparison to other industries, just slightly behind manufacturing. Not only is healthcare not immune to sexual harassment, but it is one of the industries with the most pervasive reports," she says. "Unfortunately, experts believe sexual harassment claims are significantly underreported in healthcare."

Hospitals and other healthcare employers can be held liable for sexual harassment if it is so frequent or severe that it creates a hostile work environment, Flynn explains. There also can be liability if the harassment is tied to an adverse employment decision, such as a nurse being fired, not being promoted, or transferred to less desirable shifts and assignments.

"That's when the harassment becomes illegal, and the organization can face significant liability for allowing it to happen," Flynn says. "We hear nurses say that sexual harassment is just part of the job, but employers have to actively work to change that attitude. They have to make it clear that employees have the right not to be harassed in the workplace and show them the mechanisms for reporting this behavior."

There are many possible explanations for the underreporting of sexual harassment in healthcare, Flynn says. First, nurses and other employees may be unsure of what constitutes sexual harassment, just where the line is drawn, she says. They also may feel that reporting sexual harassment will reflect badly on them and be counted against them in their workplace evaluations, Flynn says.

"The facility or organization also might not have a clear reporting policy or mechanism. So even if a nurse wants it, she might not know how to," Flynn says. "There also is the possible fear of retaliation by the person she's reporting, especially if that person is someone she works with and is in a position of authority."

Harassment in healthcare can take various forms, with an employee being harassed by a patient, visitor, colleague, or superior, Flynn says. There also can be cases in which an employee is being harassed or abused by a person he or she has a relationship with, the domestic relationship carrying over into the workplace, she says.

When patients sexually harass staff, staff members should be empowered to tell them the behavior is unacceptable. Flynn says staff members should speak directly to patients unless there is fear they will become physically abusive.

"That conversation is to set boundaries, to make clear that the comments the patient is making are unwanted. You have to be firm on that behavior, making clear that actions will be taken if that behavior does not stop," he says. "You need to make a clear record of the encounter including exactly what was discussed and any verbatim comments from the patient, along with statements from any witnesses who were present for the behavior."

If the behavior continues, the employee's supervisor should speak to the patient. Continued sexual harassment by a patient can justify transferring him or her to another facility or caregiver, Flynn says.

"Your facility should have a clear policy on sexual harassment and the means for reporting it, but it's also important that your employees model the desired behavior in front of patients and co-workers," Flynn says. "The nurses themselves should avoid using terms that are harassing or inappropriate. If they find themselves making an inappropriate comment, they should immediately apologize."

Healthcare organizations should provide annual training on sexual harassment that includes an explanation of policies and procedures, the mechanisms for reporting harassment, what will happen after it is reported, and what constitutes unacceptable behavior, Flynn says. The training might also include how to recognize warning signs of sexual harassment and assaults, and de-escalation techniques that might help defuse a situation that could lead to aggressive behavior. ■

SOURCE

- **Jennifer Flynn**, CPHRM, Manager, Healthcare Risk Management, Aon, Fort Washington, PA. Email: jennifer.flynn@aon.com.

Did ED Fail to Give Appropriate Discharge Instructions?

An ED patient was prescribed antibiotics but never filled the prescription. A few days later, the patient returned to the ED, septic. The patient sued, alleging that the EP should have admitted the patient for further evaluation.

"Even though the patient should have taken the antibiotic prescribed at the first ED visit, it would be difficult to demonstrate that negligence was related to the ED physician failing to admit the patient for further work up," says **Paul C. Kuhnel**, JD, an attorney in the Roanoke, VA, office of LeClairRyan.

This makes it easier for the EP to claim that the plaintiff failed to mitigate her damages. "Comparative negligence is available in many jurisdictions. Failure to mitigate damages, a close cousin to contributory negligence, is also available," Kuhnel adds.

Contributory negligence, in those jurisdictions that recognize it, can be difficult to demonstrate. This is because the patient's negligence must occur at or about the same time as the physician's alleged negligence. The difficulty of arguing that the patient is at fault for failing to tell the EP an important piece of history is another obstacle.

"In dealing with healthcare professionals versus a patient who may not have education beyond high school, the jury could likely conclude the physician should have elicited that history from the patient," Kuhnel offers.

Other malpractice claims have involved patients discharged from the ED with an incorrect diagnosis, such as gastroenteritis. "The ED providers do not discuss with the patient what specific symptoms the patient should look out for in order to return to the ED," Kuhnel explains. Typically, the patient is just handed a generic discharge summary that tells him or her to return to the ED if symptoms worsen. "Often, the patient does not return in a timely manner," Kuhnel notes.

It is "a must" that ED patients sign a document stating that they received discharge instructions, says **William C. Gerard**, MD, MMM, CPE, FACEP, chairman and professional director of emergency services at Palmetto Health Richland in Columbia, SC.

This document and the instructions themselves should be in the medical record. But this is not enough.

"It should be documented that the patient was given verbal instructions and that they understood them, even repeated them back," Gerard says.

The same applies to any family members or others present. "Documentation that an opportunity was provided for additional questions and that at the end of the encounter all were satisfied puts the provider on solid ground should things go awry," Gerard advises.

Gerard says that personalizing instructions generally provides more protection to healthcare workers.

At first glance, discharge instructions might appear extremely detailed, covering every possible scenario. Things quickly go wrong for the ED defense team if it is revealed the information was simply cut and pasted into the ED chart.

"Sincere instructions that turn out to be macros can cause one to question authenticity and whether it was performed at all," Gerard warns.

Some evidence suggests that patients are better able to recall videotaped discharge instructions that they viewed while in the ED.[1] "This never really caught on; but recently, a new trend is developing," Gerard notes.

Some EDs are recording the patient's discharge instructions on handheld devices, then storing them on the electronic medical record patient portal so patients can access them anytime, even on their smartphones. Documenting that this process was used can be legally protective.

"It shows care, compassion, and personalized involvement of the clinician and the patient," Gerard says. ■

REFERENCE

1. Wood EB, Harrison G, Trickey A, et al. Evidence-based practice: Video-discharge instructions in the pediatric emergency department. *J Emerg Nurs* 2017;43:316-321.

COMING IN FUTURE MONTHS

- Emergency preparedness pays off
- Discovery issues in the Digital Age
- Sexual harassment in healthcare
- Top malpractice trends

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 ReliasMedia.com to take a post-test, then select "My Account" to view your available CE activities. First-time users will have to register on the site using the subscriber number printed on their mailing label, invoice, or renewal notice.

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

4. After successfully completing the test, a credit letter will be emailed to you instantly.

5. Twice yearly after the test, your browser will be automatically directed to the activity evaluation form, which must be completed to receive your credit letter.

CME/CE QUESTIONS

1. **Which of the following is true of commercial general liability policies?**

   a. Policies never provide any coverage for losses related to cyberattacks.
   b. They may provide some coverage for losses related to cyberattacks, but one should check carefully to see what is covered.
   c. Policies always provide coverage for the majority of losses related to cyberattacks.
   d. They provide coverage for losses related to cyberattacks only if the insurer provided data security services.

2. **According to Andrew Gibbs, which of the following is true of cyberinsurance?**

   a. It tends not to be expensive in comparison to other forms of insurance.
   b. It tends to be far more expensive in comparison to other forms of insurance.
   c. Policies can be obtained with a minimal application process and little investigation by the insurer.
   d. Most healthcare organizations are denied coverage by the insurer they use for commercial general liability policies.

3. **In the Anthem breach, how did hackers gain access to the company's PHI?**

   a. An employee lost a laptop containing PHI.
   b. An employee clicked on a phishing email.
   c. Someone outside the company broke into the company's server facility.
   d. An outsider paid an employee to provide access to the network.

4. **What did investigators cite as one deficiency in Anthem's network security?**

   a. Insufficient monitoring of key logs that would have helped identity the malicious activity much sooner.
   b. Insufficient backup copies of PHI.
   c. Insufficient security of physical protections, such as locked entryways, to secure server areas.
   d. Insufficient screening of employees with access to PHI.

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

Hospital Liable for Technicians' Treatment Resulting in Child's Hypoxia

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

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

Nathan Jamieson
UCLA School of Law
JD Expected, May 2020

News: In 2006, a mother gave birth to her son at a hospital. The baby was premature but otherwise healthy. He was discharged normally 48 hours after his birth.

However, after discharge, his health quickly declined and the mother brought her baby back to the hospital. During an operation, technicians had trouble properly inserting an IV line. Once the IV was inserted, the child began to turn blue and appeared to suffer hypoxia, a lack of oxygen to the brain. This hypoxia caused the child to suffer cerebral palsy and significant cognitive impairments. The technicians delayed notifying the hospital of the child's failure to breathe in contravention of policy.

The mother and child brought suit approximately 10 years later, alleging that the hospital employees' actions fell below the standard of care and caused the child's significant injuries. The hospital maintained that it provided treatment consistent with the applicable standard of care. After a three-week trial, a jury returned a verdict for the plaintiffs of more than $130.5 million.

Background: In 2006, a baby boy was born prematurely but was otherwise healthy, and he was discharged from the hospital 48 hours later. However, his health quickly began to decline. Two weeks after his birth, the mother brought her baby back to the hospital for further testing. After an ultrasound, a physician diagnosed the infant with hydronephrosis, a urological condition that causes mild kidney swelling. The physician also diagnosed the child with lupus; however, a physical examination and ECG showed no cardiac involvement.

ONCE THE IV WAS INSERTED, THE CHILD BEGAN TO TURN BLUE AND APPEARED TO SUFFER HYPOXIA, A LACK OF OXYGEN TO THE BRAIN.

Several weeks later, the infant underwent a renal examination at the same hospital. During the examination, the technicians experienced difficulty connecting an IV line and struggled to identify a vein. Once it was inserted, the mother reported, the boy's condition worsened dramatically. The child immediately turned blue and experienced difficulty breathing. The technicians conducted mouth-to-mouth but failed to check the child's pulse or provide chest compressions. The technicians also failed to alert a Code Blue, which would have triggered a more thorough and necessary response for emergency resuscitative efforts. This would include the option of using defibrillators and other advanced technology as necessary.

The mother and child brought suit in 2016, alleging that failure to initiate a Code Blue, check the child's pulse, and provide chest compressions constituted actions below the standard of care and caused the boy to suffer a lack of oxygen and blood to his brain, creating a hypoxic ischemic injury. During trial, the plaintiffs argued that the child developed cerebral palsy several months after the negligent treatment and as a result of the inadequate care the child received. Because of the cerebral palsy and

brain damage, the child cannot walk or move unassisted and suffers significant intellectual deficiencies. The child will require significant and expensive medical care and assistance, including a full-time caregiver, for the remainder of his life as a result of these injuries and conditions.

What this means to you: A few important lessons can be learned from this case. First is the doctrine of *respondeat superior*, where an employer is liable for the actions of an employee when the actions of the employee arise during the course and scope of the employment.

Under this concept, both the employer and employee are liable for actions of the employee; however, as a practical matter, an injured party tends to seek relief only from the employer, who almost inevitably has the "deep pockets" from which to recover monetary damages. In this case, the mother and child brought suit against the hospital as a result of the actions of the technicians, who were hospital employees.

It follows that hospitals, clinics, and any care provider who is an employer must be particularly cautious and provide adequate employee training, supervision, and oversight. Doing so will help to ensure that patients are provided care within the applicable standard and, it is hoped, prevent medical malpractice claims from arising. Employer care providers should maintain thorough guidelines, standards, employee handbooks, and other relevant written documentation, and provide all of that documentation to employees.

Employers also should periodically evaluate the knowledge and efficacy of employees to ensure they have read and understood applicable policies. Annual competency evaluations of all hospital employees are required if these facilities receive government funds for services provided to patients.

While very unlikely that the insertion of the IV itself was the cause of the child's respiratory arrest, it is much more probable that the child had an anaphylactic reaction to the contrast media that was injected through the IV line. While this contrast media is used to enhance visualization of internal organs for ease of interpretation, allergic reactions to it are not uncommon.

Since, in this case, the newborn patient likely had no history of an allergy to contrast, the hospital staff had a duty to be both well-trained and prepared to respond to it. Thorough documentation of such policies and the employer's efforts to ensure employee training will serve as useful evidence if any medical malpractice case arises where an injured patient alleges that an employer's policies fall below the applicable standards of care.

Additionally, an employer may use such written policies to argue that an employee's actions deviated so significantly from those as to be beyond the scope of employment. Such arguments may be difficult to make if the employee clearly was acting with the intent to provide medical care to a patient, but having well-developed written policies and procedures in place may better substantiate such arguments.

Furthermore, having the appropriate emergency equipment available is effective only if staff members know how to use it. Facilities commonly fail to assure this. Technicians are not licensed to provide the same level of care as physicians and registered nurses, but they can be trained to perform certain procedures under the supervision of a physician or nurse. Hospitals must assure that the medical staff oversees the rules, regulations, and policies that delineate who can do what, under which circumstances and under what level of supervision. It is a complex process that can lead to disastrous outcomes when it is not well-executed.

Finally, the delay between the injury and lawsuit in this case merits discussion. While the child in this case was injured shortly after birth, litigation began approximately 10 years later — well after the child's injuries had become apparent and the child required medical care. It is not clear why the mother and child delayed filing suit, as they could have brought their claim immediately after recognizing the injury.

Nevertheless, in cases involving injured minors, the law typically permits such delayed litigation, providing additional time to file suit. This is known as "tolling," which suspends the statute of limitations until the injured party turns 18. Statutes of limitations and rules regarding tolling vary by state, but it is reasonable to believe that in cases similar to this one, many courts would allow litigation well beyond normal filing deadlines.

For healthcare providers, this may impose financial and insurance burdens beyond maintaining records and witnesses for more than 10 years. Providers and risk managers should familiarize themselves with these legal concepts, for a party injured early in life may appear many years later, and liability may still be assessed despite the passage of time. ■

REFERENCE

Decided on Sept. 24, 2018, in Oakland County, Michigan; Case Number 2016-151195-NH.

Delayed Laboratory Analysis Results in Permanent Paralysis and $44.5 Million Verdict

News: A nine-year-old boy complained of ear pain, vomiting, headache, fatigue, sensitivity to light, loss of appetite, and trouble urinating. His parents took him to a hospital for testing. Nurses undertook several tests on a STAT basis, which requires that the laboratory perform the tests and return the results within several hours; however, the lab took six days to return these results, which would show that the patient had an ear infection. During that waiting period, the boy's ear infection quickly traveled from his ear to his brain, rendering him paralyzed.

The patient brought suit against a hospital, medical associates' group, and the laboratory, alleging that each entity was negligent. A jury agreed that the providers' actions fell below the standard of care and returned a verdict for more than $44.5 million.

Background: In 2013, a nine-year-old boy was taken to his pediatric physician several times in one week, complaining of ear pain, vomiting, headache, fatigue, sensitivity to light, loss of appetite, and trouble urinating. The physician and a nurse ordered lab work to be completed on an emergency "STAT" basis because the tests were critical to proper diagnosis and timely treatment. This included an erythrocyte sedimentation rate (ESR) test and a C-reactive protein (CRP) test. According to the lab's own policies and procedures, STAT tests require that the laboratory return results within two hours. These tests were submitted at 2:30 p.m., and the results should have been returned by 4:30 p.m.

However, the laboratory failed to meet this emergency deadline and did not return the test results for six days. While the physician and family were awaiting the results, the boy's condition dramatically worsened as the infection traveled from his ear to his brain. The spread of infection caused significant and permanent injury, including permanent paralysis. When the laboratory results finally arrived, they revealed that the boy's ESR and CRP were significantly heightened.

WHILE THE PHYSICIAN AND FAMILY WERE AWAITING THE TEST RESULTS, THE BOY'S CONDITION DRAMATICALLY WORSENED AS THE INFECTION TRAVELED FROM HIS EAR TO HIS BRAIN.

The boy's family brought suit on his behalf against multiple entities, including the hospital, a medical associates' practice, and the medical laboratory. Prior to trial, the family settled with the hospital and medical practice, leaving only the laboratory as a defendant. At trial, the family alleged that the laboratory's delay fell below the standard of care because the lab owed a duty to run the tests on that same day and within two hours as required by the STAT guidelines. The lab's delay was thus the direct cause of the patient's injuries because if the lab promptly conducted the tests and provided the results, the physician would have diagnosed an infection and referred the patient for urgent treatment at a hospital.

Multiple medical witnesses and experts testified at trial, including the patient's pediatric physician and nurse, who stated that based on the test results, the patient had a likely infection requiring treatment at a hospital. By contrast, the defendant laboratory argued that it was not liable and that even if the test results would have been returned sooner, the quality and manner of care would not have changed.

The lab alleged that the delay did not cause the injury because the physician's treatment recommendations would not have been any different. One of the defendant's experts opined that lab results demonstrating elevated ESR and CRP do not require sending a child to a hospital, even with a presumed viral infection. Another expert concurred with the course of treatment and stated that the tests were not of any value in the clinical setting of the patient's illness, as the tests did not assist with diagnosis.

The jury returned a verdict in favor of the plaintiff in the amount of $24,514,226 for economic damages and $20 million for noneconomic damages, totaling more than $44.5 million. The hospital and medical associates' group settled prior to trial, and the terms of that settlement are confidential; however, any amounts the patient received from those

settlements will likely be deducted from the jury's award. The jury attributed 50% liability to the lab, 15% to the medical associates, 5% to the hospital, and 30% to a certified nurse practitioner employed by the medical associates.

What this means to you: This case serves as an example to physicians and medical providers that ordering medical tests is not a matter of order and forget. Rather, providers and laboratories must be diligent in efficiently processing tests and returning the results in a timely fashion.

While providers may feel inundated by other patients' problems, that alone is not sufficient to obviate responsibility to follow up on tests previously ordered. Medical laboratories similarly must identify that laboratories owe a duty of care to patients as well, even if the laboratory is not directly connected to the patient, as is often the case when a physician or hospital is an intermediary. Although laboratories often may appear removed from direct patient care, they are rather a crucial link in the chain that is patient treatment.

This lesson also is instructive for medical care providers who may not interact directly with patients; they still must be cautious and fulfill their duties. The physician and the nurse practitioner who were awaiting the results also had a duty to follow up with the laboratory and, if unable to obtain the results they needed, seek alternative sources of data so that the medical plan of care for the child was developed using the optimal amount of diagnostic information available.

Four different medical care providers in this case were determined to have acted negligently, and this context reveals how a jury evaluating wrongdoing may attribute percentages of liability to parties. Since the lab had the primary responsibility of performing the tests, it is unsurprising that it was determined to have the highest portion of fault, at 50%. The medical associates' group and an employee nurse practitioner had the next-highest portion of fault, and their negligent actions were predicated on the initial negligence of the laboratory — the jury found that the group and employee failed to follow up with the lab when the test results were not timely returned.

Medical care providers often have little or no option but to work with other providers in order to best provide services to patients. When such cooperation is required, it does not relieve the primary or referring provider of all liability. Instead, providers may have a responsibility to make best efforts of coordination and to follow up with the secondary or referred provider, especially for time-sensitive treatment.

In this case, the medical associates' group knew that the STAT tests were supposed to be returned within two hours, but they made apparently no effort to check on the status of the results despite the laboratory having grossly missed the two-hour requirement. When the standard of care mandates that a reasonable physician would follow up, especially for an emergent situation requiring prompt attention, failure to do so may constitute medical malpractice.

Another important lesson from this case is the option for settlement. While the plaintiff sued three different entities, two of them settled prior to trial and prior to the imposition of a $44.5 million verdict. The terms of those settlements are confidential, but given the significant size of the jury's verdict, it is likely that the settlements were much smaller. Alternative dispute resolution, such as mediation, provides a vehicle for parties to pursue settlement discussions, often with the assistance of a neutral third party who may weigh the strengths and weaknesses of cases. Care providers who have been sued should discuss these options with counsel, as settlements may provide invaluable benefits beyond strictly monetary benefits, including the prevention of widespread news coverage that inevitably occurs as a result of public multimillion-dollar verdicts.

To satisfy the duty of care, medical care providers and laboratories should consider processes and procedures to ensure that results are returned when expected. These procedures also should avoid accepting tests when the laboratory lacks the bandwidth to process them in a timely matter. However, as a practical matter and to protect against delayed tests, medical care providers and labs should prepare for such delays.

A procedure by which untimely tests are identified while still in processing and analyzed to see how long any delays are expected, or alternative options such as referring those tests out to alternate facilities for processing, will reduce potential fallout from delays. While this may seem like an onerous proposition, this case illustrates that having a substantial workload does not obviate the responsibility healthcare businesses owe to patients. ■

REFERENCE

Decided on Sept. 28, 2018, in the Franklin County Court of Common Pleas, Ohio; Case Number 14CV002543.

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Operational Issues Often Hamper Access to Patient Records

Despite warnings from the Department of Health and Human Services' Office for Civil Rights (OCR) that patients must be provided access to their medical records without undue restrictions or burdens, healthcare providers still are charging excessive amounts and making it difficult to obtain copies.

New research indicates a substantial number of hospitals are not compliant with HIPAA guidance on patient requests for records. *(The study is available to view online at: https://bit.ly/2RoS0sp.)*

Healthcare providers are not meeting OCR's expectations for patient access to protected health information (PHI), says **Harlan M. Krumholz**, MD, SM, professor in the Institution for Social and Policy Studies at Yale University.

"Patients in the real world encounter substantial obstacles and, often, costs in their efforts to access their medical records," he says. "A lot of hospital policies are out of alignment with federal regulations. There is a lot of vulnerability at these institutions that are out of alignment because they are basically violating people's rights."

> "A LOT OF HOSPITAL POLICIES ARE OUT OF ALIGNMENT WITH FEDERAL REGULATIONS ... THEY ARE BASICALLY VIOLATING PEOPLE'S RIGHTS."

HIPAA Requires Access

The HIPAA Privacy Rule states that patients can obtain copies of their medical records from their healthcare providers, and those copies must be provided no later than 30 days from when the request is made. In 2016, OCR clarified that right to access and recommended a flat fee of no more than $6.50 for providing electronically maintained medical records to a patient. The recent Yale study determined that 48 of 83 hospitals charged patients more than that, with one hospital charging a patient $541.50 for a 200-page medical record. Researchers conducted a cross-sectional analysis of medical records request processes between Aug. 1 and Dec. 7, 2017, in 83 top-ranked U.S. hospitals with independent medical records request processes and medical records departments reachable by phone. Previous research had indicated delays and high costs, but this was a larger study of prominent hospitals with robust HIPAA compliance programs.

Forty-three percent of hospitals did not state on request forms how much patients would be charged for copies of the records. Only 35% provided that information on the release form or the download webpage. Eight percent did not comply with the maximum processing time of 30 days.

OCR Penalized Hospitals

OCR has addressed these problems in the past. In 2011, it issued a $4.3 million civil monetary penalty to a hospital system in Prince George's County, MD, for refusing on 41 occasions to provide patients with a copy of their own medical records.

Some of the fault lies with overzealous compliance efforts, Krumholz says, which can happen when the organization emphasizes the consequences of improperly

releasing PHI without also educating staff on patients' rights to access their own data.

"It seems a lot of institutions are anchored in a predigital era and are unfamiliar with HIPAA rules regarding people's ability to access their own data. When someone says, *'Sorry, I can't email your own records because that would violate HIPAA,'* that's wrong. Sometimes, the patient knows that's wrong and says so," Krumholz says. "But they just tell you no. They've been so trained to comply with HIPAA that they're protecting people from their own records. That's just backward."

Krumholz recalls an incident in which a physician needed to access his own lab result for a life insurance application and used the hospital's electronic medical record to look up his own lab result.

"The institution slapped his hand for violating HIPAA," Krumholz says. "That's crazy. Just because he used the medical record instead of going through the patient portal, they said he violated HIPAA and put him on probation."

Better Education Needed

Policies and processes on HIPAA regarding patient access to records can be inconsistent even within the same institution, Krumholz notes.

"The institution might have a form for requesting records and then when you call the number on that form they tell you something entirely different," he says. "Some places also say they charge the same for digital copies as they do for paper, but of course the law says you should have a different pay structure for digital."

Krumholz recommends better education for staff on patients' rights regarding access to their records, along with a review of the processes in place that could be thwarting that access. He notes that the Health Information Technology for Economic and Clinical Health Act, which spurred implementation of electronic medical records in 2009, positively asserts people's rights to their health data.

"This is important to understand not just in terms of avoiding overcompliance, but in terms of simply complying with equally important parts of the law," Krumholz says. "The law states that you have to keep people's data safe from people who aren't supposed to see it, but it also says you must make it available to people who want to see their own data. That second part is not any less important than the first, and institutions have to start seeing that in an affirmative way." Better education of staff on this issue may not be as easy as simply explaining what the law says, notes **Alisa L. Chestler**, JD, shareholder with the Baker Donelson law firm in Nashville, TN. HIPAA compliance sometimes involves judgment calls that can be taught as black and white matters, she says. A simple request from a patient for his or her own medical record may be straightforward, but staff encounter more nuanced situations, too, Chestler says. For instance, requests for data to be used in research can be more complex.

"It's very hard to teach the staff on the frontline of these issues the smell test, how to make those calls in which a HIPAA issue is not so clear," she says. "We've all had employees who understand these issues better than others. When you're training your employees, you're going to the lowest common denominator. I have a lot of sympathy for the hospitals and understand why they say no sometimes."

The hospitals' failure to provide medical records in a timely manner, and at a reasonable cost, also may not be strictly the fault of their HIPAA compliance programs, Chestler says. Requests may be held up because of concerns over what is in the medical record, particularly if there might be litigation, she says. Those concerns do not necessarily justify a delay or trump HIPAA, Chestler notes, but they may explain how some of the problems patients encounter are not the result of overzealous HIPAA compliance.

May Be a Resource Issue

Chestler also notes that some of the problems cited in the Yale study do not appear to be related to HIPAA compliance policies.

For example, the study authors said they placed a maximum of five calls to the hospital's medical records

EXECUTIVE SUMMARY

Research continues to show that patients are denied access to medical records because of HIPAA-related restrictions and processes. Sometimes, the problem is overzealous compliance efforts; other times, it is a mundane operational issue.

- Some hospitals charge too much for records.
- HHS has clarified that patients must be granted access to their records.
- HIPAA compliance is subject to the same operational limitations as other hospital functions.

department, and the hospital was considered unreachable on each attempt if the call was not answered, went to voicemail, or an automated system did not allow the option to reach a representative. After leaving voicemail, the researchers allotted seven days to receive a return phone call. If the hospital did not return the call in that time, the hospital was classified as unreachable.

"That's not a HIPAA issue. That's a resource issue," Chestler says. "People might have that experience and blame HIPAA, or the way the hospital restricts data access under HIPAA. The reality might be that this is just about the hospital having the resources to answer phones and respond to requests."

In that regard, HIPAA compliance may not be any different than a lot of areas of healthcare, Chestler offers. Perfect compliance and customer service are admirable goals, but the realities of staffing, funding, and resources often get in the way, she says.

A good tactic may be to see HIPAA as more of an operations issue than a compliance issue, Chestler says. She notes how CMS recently pushed for healthcare organizations to get away from reliance on fax machines, especially requiring patients to fax document requests and receive documents by fax. During the Office of the National Coordinator for Health Information Technology's Interoperability Forum in Washington, DC, in August, CMS Administrator **Seema Verma** said that "one of my main missions is to break down barriers to interoperability." Health information technology remains far behind all other major industries, she added. Physicians still record their notes on paper. Often, patients are told that their data cannot be shared with another provider, or provided to them digitally, because of the fear the patient data will be intercepted by a third party, Verma said.

"We can keep data secure while making it available to patients," she offered.

Chestler says telling patients they have to send a records request by fax is "one step above telling them to hammer it out on a rock" and interferes with efforts to properly comply with HIPAA.

"The compliance team and the operations team need to have a better mechanism for communicating," she says. "People are just used to doing things the way they've always done it. The frontline staff are afraid to do it any differently for fear of getting in trouble. Nobody is pausing to ask if this is the most efficient way we can handle this issue."

One of the problems cited in the Yale study was hospitals telling patients that their records could be faxed only to a physician and not the patient. Chestler wonders why that happens in 2018 when other means of delivery are used so commonly. Still, even when that problem occurs, it is not really an issue of HIPAA compliance, Chestler notes.

"Any time someone has trouble getting their records, it is easy to assume it is a HIPAA issue," Chestler says. "HIPAA may be involved somewhere, but the real problem might be that the people in charge of HIPAA compliance created policies that made sense to them without following through with whether there are processes and resources in place in the organization to carry out those policies in an effective way. It's not enough to make HIPAA policies if you don't have a system that can do what you're requiring."

Chestler recommends reviewing HIPAA compliance with an eye toward improving the processes that underlie it. Keep in mind that the old way of handling records requests and other HIPAA matters may not be the best, she says.

"This is such a prime area for efficiencies that could save the organization money in the long run as well as improving how you comply with HIPAA and satisfy these requests," she says. "It's about being smart and going beyond the policies you put on paper." ■

Hefty HIPAA Penalties for Allowing TV Cameras in Hospitals

OCR has reaffirmed its position on television film crews in clinical care areas, issuing substantial fines on three hospitals that OCR says violated HIPAA by disclosing PHI to a broadcast news organization.

In September, OCR announced that three hospitals in the Boston area have agreed to pay a collective $999,000 to settle potential violations of the HIPAA Privacy Rule. *(The OCR announcement is available at: https://bit.ly/2pUVq9F.)* HHS alleges that the covered entities allowed television crews into patient areas of the hospitals in late 2014 and January 2015 and that PHI was not adequately protected.

This was not the first large penalty related to allowing media crews inside hospitals. In April 2016, a New York hospital agreed to pay a $2.2 million penalty and to institute corrective action plan for similar alleged HIPAA violations related to the filming of a television show. *(The OCR announcement of that settlement is available at: https://bit.ly/2ylUIqF.)*

OCR issued guidance on allowing media crews into patient care areas, specifically stating that patients must provide consent for their images and other PHI to be used before they are recorded in any way.

It is not sufficient to require the media outlet to blur or otherwise disguise the image, or to alter the voices, of patients who did not provide written authorization beforehand. *(Read much more about the OCR guidance on this issue at: https://bit.ly/2CvKhUY.)* ■

Hospital Cited for Recording Psych Patient in ED

A Minnesota hospital violated patient privacy by recording patients without their knowledge or consent during psychiatric evaluations in the ED, according to a CMS investigation.

CMS investigated the complaint of a woman who had been taken to the hospital's ED against her will in May 2017. Police took her for a psychiatric evaluation because they were concerned she might harm herself or others. She later sued the police and hospital.

In the course of litigation, the woman sought security camera footage from the hospital, which showed her changing clothes and undergoing an examination against her will.

In the CMS report, the woman expressed shock and horror that she was recorded, claiming there was no sign indicating the facility was videotaping.

In a statement, the hospital promised to cooperate with investigators while reaffirming its commitment to protect patients' rights and safety. The hospital also said it has discontinued recording but still uses the video cameras to monitor rooms for safety. Privacy screens were added to the rooms with cameras, and nurses have been trained to tell patients about the video monitoring.

CMS determined that the hospital had installed cameras to its eight psychiatric evaluation rooms because of an increase in violent incidents, with a monitor for the cameras at the nursing station. The investigation also determined that the patient intake forms included a consent form for videotaping to be used in medical education, but the woman refused to sign the forms. ■