HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE SINCE 1979

INSIDE

RELIAS MEDIA

SEPTEMBER 2020 Vol. 42, No. 9; p. 97-108

How One Hospital Screened Every Employee Daily for COVID-19

The Miami (FL) Cancer Institute achieved a feat that many healthcare institutions aspired to during the worst of the COVID-19 pandemic: screening every employee and visitor every day for COVID-19 symptoms before allowing them into the facility. The logistics may be useful to other hospitals in the next disease outbreak.

Miami Cancer Institute screens 100% of its employees because it serves a high-risk cancer population and must ensure no one is symptomatic. In some periods, they have screened 2,000 people a day with 50 staff members performing the screening process.

The effort was accomplished with support from the Baptist Health System, which coordinated the COVID-19 response for its nine hospitals, says **Michele Ryder**, MSN, MSHSA, RN, CENP, chief operating officer and chief nursing officer of Miami Cancer Institute. The health system and the Miami facility used the recommendations from the Centers for Disease Control and Prevention (CDC) and the more targeted Florida state guidelines to develop a comprehensive testing program, Ryder says.

> "WE KNEW WE HAD TO NOT ONLY KEEP OUR PATIENTS SAFE SO THEY COULD CONTINUE THEIR TREATMENTS, BUT WE ALSO HAD TO DO WELL BY OUR EMPLOYEES."

While many hospitals were moving patients out to make room for expected COVID-19 patients, Miami Cancer Institute determined it could not interrupt chemotherapy or radiation treatments. That made it one of the few facilities treating patients full time on a regular basis during the height of the pandemic, Ryder says.

ReliasMedia.com

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

HEALTHCARE RISK MANAGEMENT™

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

GST Registration Number: R128870672

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

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

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

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

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

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

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

AUTHOR: Greg Freeman
EDITOR: Jill Drachenberg
EDITOR: Jonathan Springston
EDITORIAL GROUP MANAGER: Leslie Coplin
ACCREDITATIONS DIRECTOR: Amy M. Johnson, MSN, RN, CPN

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

"We knew we had to not only keep our patients safe so they could continue their treatments, but we also had to do well by our employees," Ryder says. "If we were going to run at full volume, we had to develop a distinct screening system. We had to do it very quickly to establish a system that screened visitors, patients, and staff."

Screening and Temps

Anyone who entered the building first had to answer screening questions and take their temperature. The hospital kept a paper log of each screening until **Paul Lindeman**, MD, medical director of informatics, helped develop an electronic screening tool and log.

"We initially thought of five screening areas because we were looking at the entrances and the doors to our buildings. We quickly realized we needed to take that down to two entrances so that we would have enough screeners to last us long term," Ryder says. "It took us between 40 and 50 people every day to man these screening centers."

The screeners were selected from a wide range of employees who could be pulled from their usual work without adversely affecting patient care or overall operations of the facility, including environmental and dietary staff, she explains. They were trained on how to use the new database and ask the screening questions. The hospital developed 16 new workflows to direct them through the process.

"The workflows were reviewed daily and updated according to the most recent CDC recommendations, which was an important risk control element as well as making sure we were screening most effectively," Ryder says.

The hospital also increased the use of telehealth to reduce patient visits. Pharmacists reviewed treatment protocols, looking for any potential medication changes that could lengthen the time between patient visits, Ryder notes.

The screening was conducted from 6 a.m. to 6 p.m., with coverage for all staff and patient visits, seven days a week. Each screening station included primary and secondary areas. If an employee or visitor answered yes to a screening question in the first area, that person had to go to the secondary area for testing.

"All of these things happened between March 16 and March 30, a two-week period in which everything was transitioning very quickly at full tilt," Ryder says. "At the end of March, we implemented

EXECUTIVE SUMMARY

A hospital in Florida enacted a program to screen every employee daily for symptoms of COVID-19. Their experience holds lessons for the next pandemic.

- Everyone entering the building was processed through screening stations.
- Forehead thermometers were not entirely reliable. High readings required oral temperature confirmations.
- Staff and visitors with COVID-19 symptoms were immediately tested for the virus.

a no-visitors policy when we got to the point that we had as many visitors as we had patients. We had between 600 and 800 patients, so then we had that number of visitors, also. It was too much."

Visitors Banned

At one point the hospital was screening 2,000 people a day. Eliminating visitors helped keep the system functional and was consistent with the guidelines for social distancing, Ryder says. The hospital's patient experience staff stepped in to assist patients who arrived without the family members who might normally help them enter and exit the facility.

The hospital also used online platforms for cancer support groups and other meetings that needed to continue when visitors could not enter the facility.

Lindeman also introduced a software program to the screening stations that allowed the tracking of symptoms. "We essentially implemented an entire COVID clinic at Miami Cancer Institute. When you pull into the parking garage, someone greets you and asks you screening questions," Lindeman explains. "If you answer yes, you go to secondary screening, and if you answer no, you enter primary screening. We emptied out our cafeteria and turned it into a very structured area for our primary screening."

Double-Checking Fevers

Checking for fever was a first step. After some experience, hospital leaders determined the thermometers used for forehead temperatures were not 100% reliable. Anyone with a reading of 98°F or higher was directed to another station for an oral temperature reading. An oral reading of 100.4°F was an immediate fail. Any temperature below that allowed the person to continue to primary screening.

Any "yes" answer in primary screening directed the person to secondary screening, where advanced practice providers probed for more specific information about symptoms such as coughing.

"You're getting a provider visit right there at our on-site screening, with zero wait time. That trained medical professional is able to ferret out if this is a new cough, any changes, any reason to suspect that this could be a relative symptom of COVID-19," Lindeman says. "If the answer is yes, you moved on to our testing tent where, if you were an employee and not registered in our EMR [electronic medical record], you are registered on the spot and tested by advanced practice providers in full PPE [personal protective equipment], with a dedicated donning and doffing area."

Everyone tested is registered in the symptom-tracking software system, which includes an app downloaded on the subject's cellphone. Miami Cancer Institute uses the app to communicate with testing subjects. The app also asks the user for updates on symptoms twice a day. Negative responses sort to the top of a status board, showing hospital leaders who is not doing well and may need more attention, Lindeman explains.

Military Training Helped

Some of the success of the screening program can be traced to the military backgrounds of several hospital leaders, notes **Matt Baumann**, MBA, assistant vice president of operations and formerly with the U.S. Marine Corps. Their skill set and approach to rapid problem-solving helped the hospital launch such a large screening program in a short time, he says.

A command center provided hospital leaders oversight of the entire screening operation, Baumann explains, with Ryder at the head and functional leaders from several departments. The command center monitored all data and issued communications to staff.

The hospital's screening program was a variation on a standard rapid-response Marine Corps exercise, the evacuation of a U.S. embassy overseas, Baumann says.

"Instead of screening for American citizens vs. non-American citizens, we were filtering out the symptomatic and potentially exposed people coming to the facility," Baumann says. "One of the biggest successes for us was that our initial design became our permanent design. What we had initially on day one remained in place for the next three months, because it is a widely applicable screening process that works in different environments and with different purposes." ■

SOURCES

- Matt Baumann, Assistant Vice President of Operations, Miami (FL) Cancer Institute. Phone: (786) 596-2000.
- Paul Lindeman, MD, Medical Director of Informatics, Miami (FL) Cancer Institute. Phone: (786) 596-2000.
- Michele Ryder, MSN, MSHSA, RN, CENP, Chief Operating Officer, Chief Nursing Officer, Miami (FL) Cancer Institute. Phone: (786) 596-2000.

Common Misconceptions About HIPAA Can Threaten Patient Safety, Quality of Care

Despite years of educational efforts about Health Insurance Portability and Accountability Act (HIPAA) compliance, healthcare employees can labor under many misconceptions about what the privacy rule requires and what is and is not allowed. In addition to making daily work more difficult, these misconceptions can threaten patient safety and quality of care.

The scope of HIPAA is the root of many misconceptions, says **Stephanie Winer Schreiber**, JD, shareholder with Buchanan Ingersoll & Rooney in Pittsburgh.

"The No. 1 misconception is that all healthcare information held by anyone is protected by HIPAA. I often hear people say they know something about someone's health but they can't disclose it because it is covered by HIPAA," she says. "HIPAA only covers certain information held by a covered entity or a business associate, with some information excluded. Other than that, you may be subject to some state laws and restrictions as an employer, but HIPAA is not always applicable."

COVID-19 has raised more questions about how HIPAA applies to the use of protected health information (PHI) in telemedicine and the transmission of data through texts and other electronic communications, Schreiber notes. Although some rules were relaxed to help healthcare organizations cope with the pandemic, Schreiber says staff should understand it is not a permanent change to HIPAA.

"As providers begin to go back to whatever normal is, they need to be sure their ducks are in a row regarding things they were permitted to slip a little bit during the pandemic," she says.

Not Every Disclosure Is a Breach

Johnathan A. Rhodes, JD, counsel with Fennemore Craig in Denver, offers this list of common HIPAA misconceptions:

• A breach occurs any time PHI is improperly used or disclosed. Not all improper uses or disclosures of PHI constitute a breach, Rhodes says. The term "breach" is defined by regulation and requires a full risk analysis, including the extent risk was mitigated, and whether the PHI was actually viewed.

The definition also includes some situations that would not be considered a breach. If an improper use or disclosure is a breach, that will trigger certain reporting and notice obligations. However, that analysis should be completed before making that determination, Rhodes says.

• Release of PHI is required any time an entity is subpoenaed. You are not required to release PHI every time you receive a subpoena, Rhodes says. HIPAA permits, not mandates, that PHI is released after receiving a subpoena. However, that subpoena must meet specific requirements to comply with HIPAA before any PHI is released.

• A written statement from the patient is sufficient to release PHI under HIPAA. A written patient statement authorizing the release of PHI is not the same as a valid authorization under HIPAA, Rhodes says. A valid patient authorization under HIPAA must contain certain elements, such as a description of the PHI, and the purpose of the release. Any authorization should follow the regulatory requirements under HIPAA before PHI is released. A simple, signed statement from the patient generally is insufficient, he says.

• HIPAA is the only law that governs medical records. HIPAA generally pre-empts state law regarding privacy and security of PHI, unless the state law is more stringent than what HIPAA requires, Rhodes explains. While HIPAA will be the governing law most of the time, it is important to check state privacy rules as well.

EXECUTIVE SUMMARY

Misconceptions about the Health Insurance Portability and Accountability Act (HIPAA) continue despite years of education. Some wrong interpretations can jeopardize patient safety.

- Not every improper disclosure of protected health information qualifies as a breach.
- A patient's written statement to release data must meet certain requirements.
- HIPAA does not require retaining records for six years.

• **HIPAA requires covered entities to retain medical records for at least six years.** HIPAA does not specify a record retention requirement. Retention requirements for medical records are governed by state law, Rhodes says. Rather, HIPAA requires that all HIPAA documents be maintained for six years from when the document was created (or, in the case of a HIPAA policy, six years from when the policy was in effect). These documents include policies, authorizations, complaints, business associate agreements, and risk assessments.

Employee Health Records Are Different

One of the most common misconceptions about HIPAA is that it applies to employee health records, says **Erin S. Whaley**, JD, partner with Troutman Pepper in Richmond, VA. For a healthcare provider, it is easy to say all records relating to the health of an individual are governed by HIPAA, she says. However, if those records are held by the employer in its capacity as an employer — and not its capacity as a healthcare provider — the records are protected under employment-related laws, but not HIPAA.

For instance, if an employee submits health information to the employer to support a Family and Medical Leave Act claim, that information is not protected by HIPAA.

"Another common misconception is that if a provider is using a hosted EMR [electronic medical record], the EMR vendor will be responsible for all aspects of HIPAA security. This is incorrect for a couple of reasons," Whaley explains. "First, even though the EMR is hosted, the healthcare provider must still conduct a risk assessment. While the provider can rely on information from the vendor in that risk assessment, the provider must undertake the required analysis. Second, there are likely machines and equipment outside of the EMR that store PHI and are not managed by the EMR vendor."

For instance, copy machines are likely to store PHI and must be scrubbed before they are sold or returned to the vendor. These additional sources of electronic PHI must be counted for the risk assessment so the provider can apply proper safeguards and mitigation measures. These misconceptions can hinder patient care and interfere with healthcare operations, Whaley says.

One misconception that hinders patient care is that a patient must sign a specific form to release his or her record to another provider for treatment, Whaley says. An authorization is not required to disclose PHI for treatment.

"Sometimes, the healthcare provider adopts a policy requiring the provider's specific medical records release form to be signed. The provider tells staff that this form is required by HIPAA, but it is not," she says. "In addition, HIPAA does not require a wet signature. E-signatures are acceptable as long as they meet the applicable requirements of e-sign laws. When a provider adopts a policy requiring a wet signature from patients on the provider's specific medical records release form, this can inhibit, or at least delay, the transfer of records."

The 21st Century Cures Act regulations aimed at prohibiting information-blocking should help address provider practices that inhibit patient-directed record transfers, Whaley notes. (*More information is available at: https://bit.ly/3isu9oe.)*

Providers have appropriately trained their staff on the importance of maintaining the confidentiality and security of PHI, Whaley says, but they typically have not spent as much, if any, time training their staff on the individual rights provisions in the Privacy Rule. Healthcare leaders can remind their staff these individual rights must be respected and create realistic and workable policies to enable this compliance, she says.

"While the risk of penalties from an unauthorized disclosure is greater than the risk of penalties from violating the individual access rights by being overly strict in its application, we may start to see that balance shift. Between the 21st Century Cures Act regulations and new cases where providers are fined for not providing access, it is important that providers be prepared to respond to individual requests for access," Whaley says. "For instance, in September 2019, one hospital paid $85,000 to OCR [Office for Civil Rights] to settle a potential HIPAA violation resulting from its failure to provide records in response to a request for access." *(Find out more at: https://bit.ly/31G2p8Y.)*

No Private Right of Action

A common misconception about HIPAA is that many people believe it creates a private right of action, says **Heather Macre**, JD, director with Fennemore Craig in Phoenix. Another is that following HIPAA means one does not have to know state privacy laws.

"There also is the belief that HIPAA somehow impedes medical care by limiting communications between physicians and within health systems. These misconceptions often

lead to situations where physicians and healthcare workers do not communicate effectively with one another," she says. "Leaders can help dispel these myths by making sure that all staff are trained to implement and understand both HIPAA and HITECH [Health Information Technology for Economic and Clinical Health Act]. Education is the key."

One major misconception is HIPAA applies to all medical information and anyone who has access is restricted from disclosing it, says **Jeffrey Drummond**, JD, an attorney with Jackson Walker in Dallas.

"I've dealt with many employers, landlords, and business operators who feel that they cannot provide information to customers about tenants or employees who have tested positive for COVID-19, even though they are not a HIPAA-covered entity or business associate," Drummond says. "Many people also believe that every entity in the healthcare industry is covered by HIPAA, even though healthcare providers are only covered entities if they conduct certain HIPAA-regulated electronic transactions."

Another misconception: All uses or disclosures of PHI are prohibited unless the patient specifically consents. This misconception is particularly common within the healthcare industry among people who should know better, he says.

"Obviously, even HIPAA-covered entities may use and disclose PHI for treatment, payment, healthcare operations, and as required by law, as long as it is consistent with the covered entity's notice of privacy practices" Drummond explains. "Most of these misconceptions result in people thinking that data cannot be disclosed, or that a particular disclosure is a HIPAA violation when it's not. It certainly can interfere with care when covered entities or employees feel that they are prohibited from making a permitted disclosure, which can result in delayed or reduced care."

Avoid Overly Strict Interpretations

Regular training is the best way to keep employees from an overly strict interpretation, Drummond says. This includes training specifically when these incidents occur so lessons are learned while the situation is fresh.

One of the best ways to dispel the myths in the general public is a fully developed and plain-language notice of privacy practices, Drummond says. When patients complain that a particular use or disclosure is a HIPAA breach, the best response is to show a specific description of the use or disclosure in the notice of privacy practices.

It is important to ensure a proper understanding of HIPAA rather than letting employees err on the side of caution with an overly strict interpretation, Drummond says.

"In the most extreme example of medical record privacy, nobody will know my PHI, not even my doctor. Obviously, I'm not going to get good healthcare if not even my doctor knows what's wrong with me," he says. "On the other hand, a zero-privacy environment will necessarily result in better healthcare, since the medical industry would be able to learn everything about healthcare. Thus, perfect privacy results in bad healthcare, while the best healthcare can only occur when privacy is limited. Neither of those situations is great."

Best privacy practices must be balanced with best healthcare practices and find a middle ground, he says. Good healthcare depends on the use and disclosure of information; patients cannot be treated or cured if their care providers do not share necessary information.

"While an overly restrictive interpretation might not matter in many situations, when that interpretation becomes the norm among the staff, a patient's healthcare may suffer," he says.

Use Video Cameras

When it comes to video and privacy, there is some confusion about whether a patient's room can be on live video or if that would be a violation of HIPAA, says **Paul Baratta**, business development manager for healthcare at Axis Communications.

However, as long as the video images are protected, not publicly viewable, and the hospital informs the patient of its presence, then video is permissible, he says. Public areas like hallways, lobbies, and stairwells are not considered private areas and can be surveilled with video. One common way to ensure privacy is using patient video images in real time and not recording those images, he says.

There can be a misunderstanding of the requirements when a patient chooses to receive his or her records, says **Kevin Dunnahoo**, associate director with Protiviti, a healthcare cybersecurity company in Dallas. Many organizations believe they have to ensure the delivery mechanism of the record is secured, he says.

"The patient has the authority to authorize disclosure of their record in any means that is feasible, including unsecured transmission or storage methods like email, USBs, or CDs," he says. "While the covered entity or business associate should be

protecting these data according to HIPAA while in their custody, those requirements are done once you have the direction of the patient to disclose it if you are following their guidance and direction."

Telehealth Rules May Confuse

On March 17, OCR loosened regulations for HIPAA enforcement due to COVID-19 and the need for more telehealth services, notes **Nasir Pasha**, JD, outside general counsel with Altus Health, a concierge healthcare provider based in Santa Monica, CA. Those changes may lead to some misconceptions in the marketplace.

HIPAA still is law. OCR's reduced enforcement is mostly limited to telehealth services, he says. Another common misconception: No one is 100% compliant, and no one will ever check for compliance.

"Definitely not true. All it takes is a simple data breach or a complaint by a whistleblower that will result in an audit," Pasha says. "One of the most common misconceptions about HIPAA is that it strictly prohibits sharing of any information regarding a patient's medical condition or status. However, it is common for medical professionals to generally inform family members of a patient's medical status without violating HIPAA."

Of course, most healthcare facilities will require a patient to sign a release to share medical information to family members. This allows the patient and the facility to protect the patient's medical information, he says.

The other more common misconception is HIPAA applies only to healthcare facilities and providers. It also applies to any person who handles, stores, or otherwise has access to PHI. Covered entities are responsible for ensuring these business associates are HIPAA compliant.

"For covered entities, it is a matter of properly identifying who is a business associate and ensuring that the covered entity and business associate enter into a business associate agreement," Pasha explains. "Because of the misconception that HIPAA only applies to healthcare facilities or providers, if a covered entity does enter into an agreement with a third party that may come into contact with PHI, it's important for the covered entity to train, conduct regular audits, and have open channels for communication to prevent potential breaches."

"Leadership begins at the top. A healthcare facility or provider should have a strong compliance program and regular employee training to make sure employees, staff, contractors, and anyone else who might come into contact with PHI understand that they have a responsibility to protect PHI," he continues. "A strict interpretation of HIPAA might better protect PHI, and it is important for employees to

STEPS TO IMPROVE HIPAA COMPLIANCE AT HOME

Health Insurance Portability and Accountability Act (HIPAA) compliance for employees working remotely depends on a sound IT infrastructure. **Raghunath Thummisi**, Global Cybersecurity Market Strategist at Radware in Mahwah, NJ, offers these suggestions:

- Ensure all configurations and setup of remote equipment, software, and hardware accessing the organization's systems are performed by the IT team in a structured way. This includes setting up firewalls, antivirus software, and VPN access.
- Set up all remote employees with correct access and privilege levels based on their roles and responsibilities.
- Ensure employees' home routers are encrypted and the default passwords are changed.
- Mandate end-to-end encryption and protection of remote devices, home network, and applications, including secure transmission of patient records.
- Enforce strict acceptable usage policies and confidentiality of remote devices.
- Mandate remote employees to prevent unauthorized access at home.
- Require remote employees to follow a data confidentiality and privacy policy for document management of physical and digital documents.
- Periodically audit remote employees to ensure adherence to remote access policies. ■

SOURCE

- Raghunath Thummisi, Global Cybersecurity Market Strategist, Radware, Mahwah, NJ. Phone: (201) 512-9771.

know where and when they can share PHI and when they cannot."

One of the more common HIPAA breaches is unintentionally releasing PHI, such as discussing a patient's medical condition where others can overhear, or gossiping, Pasha notes. Avoiding that may seem like common sense, but both are violations of HIPAA and could easily occur.

"However, if employees are discussing a patient's medical condition as part of providing medical care, then that would be proper," Pasha says. "This goes back to properly training employees to understand the difference."

BAA No Panacea

HIPAA has been in place for about 14 years. Since then, "HIPAA" has entered popular culture as a synonym for all things related to healthcare "privacy," notes **Bob Dupuis**, vice president of enterprise architecture and security at Arcadia, a population health management services company in Boston.

But while HIPAA requires healthcare organizations to develop and maintain procedures to protect patient information, compliance is only the ground floor. HIPAA compliance does not mean you have what is needed to fully protect patient information from the ever-changing threat landscape, he says.

Many leaders in healthcare organizations who share patient information with third-party vendors think the business associate agreement (BAA) is all that is required to protect an organization from harm should their business associate experience an issue, Dupuis says.

"This just isn't true. There needs to be more than just an agreement on what would happen should an issue occur," he says. "A robust BAA is an important legal control, but it is only a backstop. The BAA does not provide any practical security protection for protected health data, nor does it offer any trusted third-party assurance that a vendor has end-to-end security safeguards in place to protect against both known and unknown threats."

Organizations need to ensure their partners/vendors use a strong program and controls required to protect their patient information, he says. Ideally, this assurance happens through a strong third-party program that either validates the controls via a sometimes-cumbersome vendor risk management process or requires vendors maintain a robust certification, such as HITRUST.

"The lack of strong, consistent, validated controls within healthcare information technology leads to high-profile, reportable breaches that erode trust throughout the healthcare system. This hinders the kind of data-sharing required to drive true change in population health and success in value-based programs," he says. "The misconceptions around data-sharing result in a similar slowdown of the adoption of new technologies that, if implemented effectively, could drive the change needed in the overall system: higher-quality, better-value care."

Tech Acquisitions Can Suffer

Misconceptions about BAAs often arise when a healthcare organization is acquiring technology, Dupuis says. The process for selecting technology typically is driven by the features and functionality, with security as a component but not a priority.

Healthcare organizations undergoing a vendor selection process already are performing an exhaustive amount of work to conduct a comprehensive feature-function analysis of each potential product. Additional evaluation of a vendor's cybersecurity credentials can be complex and labor-intensive, he notes.

There are many potential frameworks and controls to use. Validation of a vendor's capabilities can require substantial effort from an organization's security experts. A healthcare organization may not be able to confirm a vendor has the controls they say they do — and may struggle to measure one vendor against another when evaluating commitments to data security, Dupuis says.

"This is where certification programs like HITRUST can be really helpful. The HITRUST CSF framework incorporates existing, globally recognized standards, regulations, and business requirements, including ISO, NIST, PCI, HIPAA, and state laws. To earn certification, vendors are audited by a third party to ensure they comply with hundreds of controls," he explains. "If a vendor is HITRUST CSF-certified, a healthcare leader who may not be an expert in information security can be confident they are doing business with a partner who has independently verified end-to-end data security."

Managing the needs of a population — and the needs of the individual patients within that population — requires access to information about services patients are receiving across the care continuum, from emergency departments (EDs) to specialist care and home health, Dupuis says.

"If HIPAA is perceived to be a barrier to sharing data, that misperception can prevent providers from identifying preventive care needs or ensuring patients who visit the ED receive the appropriate follow-up care," he says. ■

SOURCES

- **Paul Baratta**, Business Development Manager for Healthcare, Axis Communications, Boston.
- **Kevin Dunnahoo**, Associate Director, Protiviti, Dallas. Email: kevin.dunnahoo@protiviti.com.
- **Bob Dupuis**, Vice President, Enterprise Architecture and Security, Arcadia, Boston. Phone: (781) 531-9129.
- **Heather Macre**, JD, Director, Fennemore Craig, Phoenix. Phone: (602) 916-5396. Email: hmacre@fclaw.com.
- **Johnathan A. Rhodes**, JD, Fennemore Craig, Denver. Phone: (303) 291-3210. Email: jrhodes@fclaw.com.
- **Nasir Pasha**, JD, Outside General Counsel, Altus Health, Santa Monica, CA. Phone: (310) 452-1800.
- **Stephanie Winer Schreiber**, JD, Shareholder, Buchanan Ingersoll & Rooney, Pittsburgh. Phone: (412) 392-2148. Email: stephanie.schreiber@bipc.com.
- **Erin S. Whaley**, JD, Partner, Troutman Pepper, Richmond, VA. Phone: (804) 697-1389. Email: erin.whaley@troutman.com.

Reduce Workers' Comp Costs with In-House Services, Return Programs

Controlling workers' compensation costs is challenging for any employer, and healthcare employers face difficult work-related situations. Paying attention to some of the most common and costliest risks can help manage the financial effects.

As many hospitals have a large deductible, or self-insure their workers' compensation exposure, the largest expense typically is their actual losses, notes **Joe Levy**, senior vice president with Risk Strategies, a consulting firm in Philadelphia.

This creates significant opportunities for a hospital that develops and manages a robust risk management program, he notes. The hospital can reduce its expenses by preventing and reducing claims through creating a culture of safety, implementing robust risk control initiatives, and using a proactive claims-handling program aimed at minimizing an injured worker's time out of work, he says.

"Some of the most successful programs implemented by hospitals to reduce injuries and the resultant costs include management leadership and support, consistent education and training, safe lifting techniques, accident investigation/injury review processes, and a transitional return-to-work program," Levy explains.

A transitional return-to-work program should include contact by the hospital's designated claims staff and/or management designee to express compassion and encourage recovery, Levy says. The goal should be 100% of injured employees returning to light duty at the first opportunity, including a light duty list of functional work tasks.

"With a program that has the commitment of leadership, the right champions internally, and accountability, you can really drive down expense, and all that flows to the bottom line," Levy says. "If you have a hospital that averages $1 million a year in claims and you can cut 20% to 50% of that, that's $200,000 or $500,000 that now is found money. Ideally, you could reinvest some of that back into the program to improve the results even more."

Top Three Injuries

The top three categories of injuries in healthcare are musculoskeletal/ergonomic injury, slip/trip/fall, and needlestick injuries, both in frequency and severity, says **Audrey Allsopp**, claims consultant and the national workers' compensation practice leader at Conner Strong & Buckelew, a risk management, insurance, and employee benefits broker in Camden, NJ.

EXECUTIVE SUMMARY

Workers' compensation costs can be controlled with a robust risk management program. A comprehensive return-to-work program is essential.

- Needlestick injuries are frequent but do not often lead to disease.
- Healthcare employers can use their own services for physical therapy and other expenses.
- Safety training should target specific hazards.

"While needlestick injuries can be frequent, they are not usually high-cost items unless they convert to disease, which is, thankfully, relatively rare. For this reason, we regularly focus on how to decrease the frequency of the first two: musculoskeletal/ergonomic and slip/trip/fall injuries," Allsopp says. "With each of these, targeted, deliberate programs have the biggest impact. Information and training are essential in fostering change, but just tossing out some information on a flyer or in an occasional training rarely get any long-term traction and results. A more deliberate training program is needed."

Medical and indemnity costs resulting from musculoskeletal/ergonomic injuries, including urgent care, diagnostic, physical therapy, and surgery, can be significant, Allsopp says. Many of these injuries are affected by comorbidities, age, physical activity, health, partnership with the specialist's community, availability of transitional work programs, and engaged partnership with the hospital workforce.

Needlestick Protocols Needed

Although needlestick injuries do not always result in infection, they must be addressed carefully with a comprehensive program, says **Melissa Zaslow Burke**, PharmD, vice president at AmTrust Financial Services in Southington, CT. Create protocols to ensure employees can be provided immediately with the necessary medications when a needlestick is reported, she says.

"This will require prior arrangements with your insurance carrier to allow the provision of those medications without any delay caused by prior authorization requirements or other limitations," she says. "We also want to ensure the employee feels supported and understands the process and expectations that go with that workers' comp injury."

Burke encourages risk managers to stay current with new technology and techniques to reduce needlestick injuries. It also is important to support the employee to reduce anxiety.

"We know that worry and anxiety can lead to elements that increase the cost of a claim, like obtaining representation," Burke says. "It's important to have protocols in place prior to needlestick injuries occurring that address not only the clinical needs but also the kind of emotional support these employees will need to get through the experience in the best way."

Use Your Own Services

Hospitals can lower medical costs through existing structure such as providing first aid, urgent care, surgery, diagnostics, physical therapy, and other on-site medical treatment, Allsopp says.

"Hospitals should partner with their claim processing partner to re-price medical bills to workers' compensation-allowed charges," Allsopp says. "The hospital is able to control medical and offer the best care to their employees by utilizing internal resources and write off medical cost at state-allowed charges."

Safety training programs should bring all parts of the organization to bear on the specific issue, she says. For example, one hospital system she worked with created a slip/trip/fall program that focused on recognizing and abating specific hazards across the hospital facilities. Since most of these hazards can be resolved quickly on the spot, the goal of the program was to develop and foster a culture where all employees think "If You See Something, Do Something" regarding slip/trip/fall incidents.

"The program revolved around training all employees about how to recognize slip/trip/fall hazards, reporting them at daily safety huddles, and providing incentives and tight accountabilities for abating the hazards once reported," she explains. "With every employee on the lookout for issues and systems to eliminate them, the facility has the best chance of abating this extremely common and often costly category of injuries. This approach is vastly different than just putting out a flyer of information, and vastly more effective."

Wellness programs that help mitigate comorbidities, such as diabetes, smoking cessation, weight, and stress management, allow employees to heal and recover faster, Allsopp says. The programs also allow employees to pursue surgery at the time prescribed rather than wait for the completion of a wellness program, which could take six months to a year, she says.

Engaged relationships with the medical specialty community such as orthopedics, neurology, and other specialists help the team understand the type of transitional work availability, Allsopp says. Invite the specialist to tour the hospital so the specialist can view the jobs, see how the job is performed, and write restrictions accordingly, she advises. The specialist can see ergonomic risk factors or controls the hospital has implemented to combat these risk factors.

"Identify transitional duty jobs prior to the work injury through engagement with insurance,

risk management, risk control, operations, human resources, physical therapists, legal, and the medical director ensures minimal down time for the employee, keeps the employee connected to the workplace, and fosters the healing process," she adds.

Tried-and-true workers' comp methods are the best avenues for minimizing costs, Allsopp says. Such methods include good incident investigation and reporting; quick, quality medical care from healthcare professionals who genuinely understand workers' compensation issues; strong and appropriate follow-up with the employee; and good return to work policies and procedures, she says.

"Engaging the hospital medical director in the claims management process is key. The medical director can oversee the medical treatment on- and off-site, assign and review restrictions, demonstrate to the employee how to perform the job duties within the restrictions, share their medical expertise in the claim review process, and build relationships with the specialist community," she says. "The common denominator among prevention, remediation, and cost/claim management is engaged, focused, deliberate, systems-oriented actions and relationships." ■

SOURCES

- **Audrey Allsopp**, Claims Consultant, Conner Strong & Buckelew, Camden, NJ. Phone: (877) 861-3220.
- **Melissa Zaslow Burke**, PharmD, Vice President, AmTrust Financial Services, Southington, CT.
- **Joe Levy**, Senior Vice President, Risk Strategies, Philadelphia. Phone: (800) 508-1355.

Prosecutors May Look for COVID-Related Restructuring Fraud

Risk managers should be on the alert for fraud and abuse related to reimbursement issues and financial restructuring related to the COVID-19 pandemic, says **Michael F. Ruggio**, JD, partner with Nelson Mullins in Washington, DC.

Many hospitals and large healthcare providers are facing massive financial restructuring or insolvency while also dealing with healthcare fraud because of the COVID-19 pandemic. With the high reimbursement rates for a COVID-19 diagnosis for hospitals ($13,000) and an additional large sum for the use of a ventilator ($39,000), the potential for fraud and abuse in hospitals is substantial, Ruggio says.

"Unless a system or careful review with proper documentation and checks and balances is developed and maintained, this could be low-hanging fruit for the Department of Justice and HHS-OIG [Department of Health and Human Services Office of Inspector General] investigations and prosecutions," he explains.

Hospital restructuring from the operations side also is needed. With ambulatory centers cutting healthcare costs, the massive expansion of telehealth services, and the rapid increase in durable and non-durable medical supplies costs, hospitals could be stuck with either a large oversupply of product or supply chain interruptions, Ruggio says.

"This situation and the rapid expansion of COVID-19 cases requires hospitals to completely restructure operations to enable them to position their supplies, supply chains, and sales forces to scale with the new and different demand for healthcare services that is developing," he says. "To fail to do this and retool appropriate governance and operations in this regard will be the beginning of the end for many hospitals and large healthcare providers." ■

SOURCE

- **Michael F. Ruggio**, JD, Partner, Nelson Mullins, Washington, DC. Phone: (202) 689-2868. Email: mike.ruggio@nelsonmullins.com.

HEALTHCARE RISK MANAGEMENT™

CME/CE INSTRUCTIONS

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

1. Read and study the activity, using the provided references for further research.
2. Log onto **ReliasMedia.com** and click on My Account. First-time users must register on the site. Tests are taken after each issue.
3. Pass the online test with a score of 100%; you will be allowed to answer the questions as many times as needed to achieve a score of 100%.
4. After successfully completing the test, your browser will be automatically directed to the activity evaluation form, which you will submit online.
5. Once the completed evaluation is received, a credit letter will be emailed to you.

CME/CE QUESTIONS

1. **How many staff members are required to screen everyone entering the Miami (FL) Cancer Institute for COVID-19 symptoms?**

   a. 10-20
   b. 30-40
   c. 40-50
   d. 50-60

2. **The screening program at the Miami (FL) Cancer Institute was modeled on what kind of emergency response?**

   a. A natural disaster, such as a hurricane
   b. A fire at the hospital
   c. A terrorist attack in the community
   d. A U.S. embassy evacuation

3. **Audrey Allsopp notes the top three categories of injuries in healthcare are musculoskeletal/ergonomic injury, slip/trip/fall, and:**

   a. needlestick injuries.
   b. hospital-acquired infections.
   c. traumatic injuries.
   d. burns.

4. **Which is true regarding HIPAA and subpoenas?**

   a. You are required to release PHI any time you receive a subpoena.
   b. HIPAA permits, not mandates, that PHI is released after receiving a subpoena.
   c. Any subpoena is sufficient because there are no specific requirements to comply with HIPAA before any PHI is released.
   d. A subpoena is never required for the release of PHI.

CE OBJECTIVES

Upon completion of this educational activity, participants should be able to:

1. describe the legal, clinical, financial, and managerial issues pertinent to risk management;
2. explain the impact of risk management issues on patients, physicians, nurses, legal counsel, and management;
3. identify solutions to risk management problems in healthcare for hospital personnel to use in overcoming the challenges they encounter in daily practice.

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

Appellate Court Denies Attempt to Vacate $8.3 Million Birth Injury Award

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

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

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

News: A physician improperly delivered a child, causing permanent injuries, including impairment to the development and use of the child's right shoulder, hand, and arm. The patient filed a malpractice suit, and a judge awarded the patient $8.3 million in damages.

The clinic appealed, arguing the damages calculation was based on the unsupported assumption the child could have earned $100,000 per year with only a high school education. However, the appellate court rejected the clinic's arguments, finding the trial court had the discretion in determining comparative cases, and confirmed the award.

Background: During her fourth pregnancy, a patient received medical services from an obstetrician employed by a federally funded clinic. The obstetrician had not been involved in the prenatal care or delivery of the patient's first three children. Although the patient did not experience complications with her first three pregnancies and deliveries, her second son was macrosomic, or above the average weight range.

ALTHOUGH THE PATIENT'S OBSTETRICIAN KNEW THE PATIENT WAS AT HIGH RISK OF A COMPLICATED DELIVERY DUE TO MACROSOMIA, THE OBSTETRICIAN FAILED TO APPROPRIATELY MANAGE THE PREGNANCY.

Macrosomia is a particularly dangerous condition that significantly increases the chances of shoulder dystocia, a condition in which the child's head is delivered but the shoulders remain stuck in the birth canal. This condition often leads to permanent injuries to the child's shoulders, arms, or brain due to nerve damage or oxygen deprivation. Furthermore, the risk of shoulder dystocia is directly proportional to the macrosomic child's weight. Pregnant women who go through difficult deliveries due to this condition are more likely to experience complications during subsequent deliveries. The condition is considered a medical emergency during delivery. It is important for an obstetrician to screen for this condition and accurately estimate the baby's weight.

Although the patient's obstetrician knew the patient was at high risk of a complicated delivery due to macrosomia, the obstetrician failed to appropriately manage the pregnancy and advise the patient that a cesarean section would be a safer option. The obstetrician used a method of estimating the fetal weight that he learned during residency. This method, which was not recognized by the medical profession and had not been published or validated in any way, led the obstetrician to estimate a weight that was more than three pounds lower than the actual weight of the fetus at birth.

During delivery, the patient suffered severe complications. The obstetrician used a vacuum extraction, delivering the baby's head while his shoulders remained stuck in the birth canal. Although the nursing staff performed several maneuvers, delivery only occurred when a different obstetrician intervened after nine minutes of dystocia. The child

was blue and did not have a heartbeat at birth. Because of the significant complications, the child had to spend several weeks in neonatal intensive care. The child suffered permanent injuries to his right arm, hand, and shoulder, primarily because the nerves in his right arm had been completely torn away from his spinal cord.

The patient filed a malpractice lawsuit against the obstetrician and the clinic, alleging the obstetrician's actions constituted malpractice and caused the child's permanent injuries. The defendants denied liability.

At a bench trial, the judge ruled the obstetrician had acted with negligence and breached his duty of care. The trial court awarded the patient $8.3 million in damages, with $2.6 million constituting lost earnings, assuming the child could have earned $100,000 annually in a skilled trade with no injury and only a high school education.

The defendants appealed, arguing the trial judge should have compared the case to other cases that involved smaller non-economic awards. The defendants did not dispute liability, and instead focused their appeal on the damages calculation. However, the appellate court affirmed the award, finding the damages calculations are inherently difficult when speculating about a five-year-old's future. Nevertheless, the appellate court ruled the trial court properly evaluated the damages and correctly compared similar cases.

What this means to you: This case reveals lessons about both liability and damages, including the inherently speculative nature of damages for injuries caused to young individuals. In this case, the injuries occurred during birth. With dramatic birth injuries, an individual's entire course of life may be altered because of a physician or care provider's negligence. That can carry dramatic financial consequences. Severely injured patients may require constant medical care, may live shorter lives, or may be unable to join the workforce (or join with reduced capacities) as adults. Here, the parties disputed, and the court was required to resolve issues about the extent of the patient's physical injury on the ability to work.

THE DEFENDANTS DID NOT DISPUTE LIABILITY, AND INSTEAD FOCUSED THEIR APPEAL ON THE DAMAGES CALCULATION.

On the more substantive aspects of malpractice, this case warrants a brief discussion about how preventing such an injury may be implemented: by creating a team trained to deal with shoulder dystocia. Not all dystocia deliveries require a cesarean section, but all potential high-risk deliveries require an experienced team capable of managing a shoulder dystocia. The estimate of fetal weight is an important indicator of potential dystocia; accordingly, assuring the estimate is as accurate as possible is critically important. Guidelines from the American College of Obstetricians and Gynecologists for both the weight estimate and managing the shoulder are the gold standard in the United States. The facility where this occurred employs a medical staff responsible for selecting and credentialing new employees. This would include proctoring for high-risk deliveries to ensure a more experienced physician will attend the high-risk deliveries and be available to step in immediately if the primary physician needs assistance.

For the legal implications and damages on this case, the appellate court considered two main areas of focus. First, the appellate court evaluated the trial court's methodology for calculating damages; second, the appellate court analyzed whether the trial court abused its discretion in applying this methodology. At trial, both parties offered opinions of vocational experts who presented different methodologies in assessing the child's lost wages. While the patient's expert opined that with a high school diploma, the child would have average annual earnings of about $35,000 (approximately $5,000 less than if he had not suffered any injuries), the physician's expert claimed the injury would only affect the child's ability of working certain types of occupations involving manual labor. In particular, the physician's expert noted since the child's cognitive functions were normal, it was likely the child would complete college and could successfully perform many sedentary or knowledge-oriented careers, with an average annual earning capacity of around $100,000.

The trial court more closely agreed with the physician's expert. It found the injury would affect the child's earning capacity. In calculating lost earnings, it considered the physician's proffered figures, which argued the child may not successfully complete college, thus losing potential earning capacity of $100,000 per year. Due to his injury, the child would be unable to perform manual labor, thus losing the earning capacity of $30,000 per year.

On appeal, the defendant argued any method employed to estimate a

five-year-old's future earnings would be inherently arbitrary, and thus no financial amount could be reasonably awarded. However, the appellate court reiterated this approach would violate state law and found the trial court's calculation method and award did not constitute an abuse of discretion. The appellate court noted there is an inherent problem in calculating a five-year-old victim's expected compensation. Nevertheless, such difficulty does not justify an award of zero, especially given the fact that state law specifically provides for a showing of permanent injury and of loss earnings to a degree of reasonably certain truth.

Physicians and care providers are well advised to thoroughly evaluate the extent of the patient's purported injuries and the associated damages, as challenging the amount of damages is a ripe area for appeals. ■

REFERENCE

Decided June 30, 2020, in the United States Court of Appeals for the Seventh Circuit, Case Number 19-3071.

Appellate Court Vacates $1.1 Million Sinus Surgery Verdict for Lack of Evidence

News: A patient underwent sinus surgery that left her with a permanent loss of smell, an altered sense of taste, and other injuries. The patient filed a malpractice lawsuit, alleging the physician failed to inform the patient of a dural patch placed during the surgery, and otherwise acted negligently during the procedure.

At trial, the patient was awarded $1.1 million. The defendant appealed, and the appellate court vacated the verdict due to lack of evidence connecting the injuries to the failure to inform the patient.

Background: In February 2007, an otolaryngologist performed an endoscopic sinus surgery on a patient suffering from chronic sinusitis. The physician placed a dural patch to reinforce the patient's bone after noticing significant thinning of a bone in the patient's sinus cavity. After surgery, the patient complained about losing her sense of smell and taste. Shortly after, the patient underwent a second surgery from a different physician to drain a mucus-filled cyst in the sinus cavity and to repair the area where the other physician applied the dural patch.

The patient claimed to have suffered permanent loss of taste and smell caused by the surgeries. After the second surgery, the patient brought a malpractice lawsuit against the initial physician, alleging the physician breached her duty of care in the preoperative care unit during and after the operation. Specifically, the patient alleged the physician departed from accepted medical practices by suggesting the patient undergo a functional endoscopic sinus surgery, and the patch had caused the patient's injuries.

The defendant physician denied liability, alleging the patch was necessary to reinforce the patient's weakened bone. The physician did not dispute that she failed to inform the patient of the patch, but argued the failure to inform did not cause any injuries.

A jury found the physician had not breached her duty of care in the patient's preoperative care, had adequately informed the patient as to the risks and benefits of the surgery, had obtained informed consent from the patient, and had performed the surgery in accordance with the accepted medical standard. However, the jury found the physician departed from the accepted medical practice in failing to inform the patient of the insertion of the dural patch. Furthermore, the jury found the physician was negligent in explaining the necessary postoperative care. According to the jury, these breaches caused the patient to suffer injury requiring a second surgery. In particular, the physician did not advise the patient to stay on bed rest after the surgery to allow the dural patch to properly heal into place.

Because of the physician's failure to adequately inform the patient about postoperative care, the patient did not remain in bed and the movement dislodged the patch, causing the cyst and the subsequent injuries to the patient's senses. The jury returned an award in favor of the patient for $1.1 million. The defendant appealed.

The appellate court vacated the judgment, noting no evidence had been presented during the trial to support a verdict for the plaintiff. Specifically, the appellate court explained while the physician was negligent in the postoperative care instructions, the patient failed to present any evidence the dural patch had shifted post-surgery, causing the patient's injuries. Additionally, although the patient argued the physician should have ordered a CT scan after the surgery, there was no evidence the outcome would have

been any better for the patient. As such, the decision was reversed and the award vacated.

What this means to you: This case demonstrates the importance of carefully preparing one's argument and presenting the evidence to support necessary findings. Another interesting lesson from this case is on the basic elements of medical malpractice: Even in the face of an undisputed breach of the standard of care, medical malpractice liability is not guaranteed. A breach of the standard of care is only one element. Here, the physician did not dispute that element — she acknowledged she failed to inform the patient about the placement of the patch — but instead focused the challenge on other necessary elements, including causation. Medical malpractice only arises if a physician breaches a duty and that breach is a substantial factor in causing a patient's harm. Thus, if a patient suffers no harm, or if some other event causes the harm, the physician bears no liability.

Although the plaintiffs tried to argue the physician breached the medically accepted standard throughout the treatment, the lower court jury found the only breach occurred after the surgery, when the physician failed to inform the patient of the dural patch and provide postoperative care instructions. Physicians and care providers are required to provide clear details of findings and care provided during surgery. Any implanted materials must be disclosed to a patient, and the information about the implant, including registration or lot numbers, should be given to the patient and documented in the patient's records. Discharge instructions also should be documented as received and understood by the patient. The patient's expert opined that after the surgery, the physician should have given the patient written instructions specifying the patient should be confined to bed rest to avoid dislocation of the patch.

However, the appellate court noted the patient never presented evidence showing the patch had shifted, thus causing the injury. Without such evidence, the patient failed to satisfy her burden of proving the case. In this case, the court reiterated the patient's expert will not need to quantify the degree to which the negligence contributed to the injury, but it would be sufficient to present evidence that would lead a jury to infer the physician's conduct reduced the patient's chances of a better outcome and increased the patient's injury.

Based on this standard, the patient completely failed to show how the physician's not advising the patient as to the dural patch or the required bed rest caused the patient's loss of smell and taste, caused the mucus-filled cyst, and required the second surgery. Instead, the patient focused on presenting evidence that would support a finding of negligence during the preoperative care and the surgery itself. The jury rejected both arguments, finding the physician was not negligent before or during the surgery. Because the patient brought the medical malpractice action alleging several breaches, the evidence focused on proving the injury and failed to address how each alleged breach caused the injury.

The patient's failure in this case proved fortunate for the defendant physicians, and serves as a lesson for clinicians. This is particularly true when a patient takes a "shotgun" approach to medical malpractice liability: This patient did not pinpoint the purported negligent action, and instead broadly alleged the physician breached at times before, during, and after the surgery. Clinicians should evaluate such broad claims with particular scrutiny, as it may indicate general weaknesses in the patient's case. Undermining each alleged breach and disconnecting those from any purported injuries can be a successful method for achieving a defense verdict. ■

REFERENCE

Decided July 1, 2020, in the Supreme Court of the State of New York Appellate Division, Second Judicial Department, Case Number 2017-03518 801/12.

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

HIPAA Compliance a Concern as Working from Home Becomes Norm

Working from home is the new normal and will be for many healthcare employees for a while, so adjustments are necessary to maintain compliance with HIPAA. Protected health information must be managed properly whether the employee is in the healthcare facility or at home.

Most healthcare providers should have crafted compliance programs for remote employees before the advent of the COVID-19 pandemic. Certainly, the pandemic has pushed the urgency of such plans to the forefront, says **Richard J. Tarpey**, PhD, assistant professor in the Jones College of Business at Middle Tennessee State University.

"In my prior practitioner healthcare career and leader of Sarbanes-Oxley and HIPAA compliance programs in the past, I can say that compliance is not flexible based on the location of the workforce. It is absolutely reasonable to expect the same level of security for remote workers as is in place for employees on company property," he says. "There are several examples in the last few years of healthcare providers being held financially accountable due to the loss of PHI [protected health information] data by remote employees."

The first step is for companies to completely understand which employees have remote access, Tarpey says. Existing remote access should be reviewed and reaffirmed to those employees with valid business justification. Companies should require, and employees should be willing to sign or reaffirm, confidentiality and HIPAA compliance documents. "It is a good idea to refresh the employee obligations in the employees' minds at this time," Tarpey says.

Compliance documents should highlight policies prohibiting using company-issued devices for non-company-related work, as well as preventing non-employees from using company-issued devices or using any personal devices that connect to company networks. Also underscore the importance of properly storing PHI-sensitive printed documents, and logging off all systems after finishing work.

Policies should clearly state the consequences of violation, Tarpey says. It also is a good idea to provide refresher information for employees on printing documents at home that contain PHI information. If reasonable, companies can consider providing HIPAA-compliant shredders for employees' use at home. Alternatively, companies can create structured processes for employees to drop off printed documents no longer needed at the company location via social distancing-safe processes.

On the technology side, companies should require remote employees to use a VPN to access company infrastructure when working remotely. Also, ensure the encryption of home wireless router traffic with secure (not default) passwords. Companies can best control access by issuing remote employees who access PHI a company-owned device that is encrypted and password-protected.

"The best [tactics] are to have strong remote work and data access policies, signed HIPAA compliance documentation for each remote access worker, and robust device management policies for any device connecting to the company network," Tarpey says. "While risk mitigation of a PHI data breach can never eliminate the risk with remote employees, the key determining accountability factor in the eyes of [Health and Human Services] is how well the company has managed system access, data access, system-connected devices, encryption, and employee policies."

The COVID-19 pandemic has prompted healthcare providers to ramp up work-from-home programs for non-clinical staff, often for the first time, and certainly at a scale not seen before, says **Rich Temple**, vice president and chief information officer at Deborah Heart and Lung Center in Browns Mills, NJ. "I think all providers need to operate from the premise that the level of cybersecurity protection

provided in a work-from-home environment can be no less than what it would be in an on-site working environment," Temple says. "The consequences of data breaches and security lapses, if anything, are greater in a work-from-home environment, since the control of who is seeing what is reduced when working in a household environment. The negative consequences of breaches are still the same, regardless of where the breach originated."

With a VPN, users go through the same, secure tunnel that allows IT teams to know exactly what volume of users are on what systems at different times. IT teams can allow "one-stop shopping" reporting on security red-flags, such as multiple failed log-in attempts or unusual access patterns (e.g., logging into systems at unusual days or times for particular users), Temple notes. The single point of entry also facilitates appropriate access to only the systems an individual needs to perform his or her job.

Another highly desirable protection to put in place, if at all possible, is two-factor authentication (2FA), Temple says. Instituting 2FA largely mitigates the risk of someone using a shared or otherwise purloined password to gain access to a system to which they are not entitled.

"The virtual desktop infrastructure [VDI] environment we have rolled out here at Deborah Heart and Lung allows us to greatly reduce our exposure to any malware issues that may reside on a user's home computer. [It] also minimizes the potential for data loss, [losing] electronic protected health information [ePHI], or [misplacing] other proprietary data assets," Temple says. "When a user logs into our environment, they are presented with a containerized, segregated virtual desktop ... our environment does not allow any sharing of programs or data between the home computer and the user's isolated VDI session."

The worst-case scenario is anything installed on the virtual desktop is destroyed when the virtual desktop logs itself off after a prescribed period and will not cross over and pose a risk to other users' virtual desktops, Temple explains.

Another issue is the "paper" component of individuals' job duties, Temple says. In an office, paper containing PHI can be stored in a desk at a cubicle. With good "HIPAA hygiene," one can protect this information from unauthorized eyes. However, with employees working from home, provider organizations lose those structural safeguards. It becomes much harder to ensure family members or others do not see PHI lying on a coffee table.

Printing PHI should be sharply restricted, if not prohibited altogether, for employees working at home, says **Janet Hunt**, senior director of IT user support at Apria Healthcare, a provider of home respiratory services and medical equipment based in Lake Forest, CA. Apria employees have worked remotely to an extensive degree long before COVID-19. Hunt says restrictions on printing PHI are a necessary part of HIPAA compliance.

"It's impossible to know where that PHI goes once it's printed on paper. We can't have it sitting around someone's home for just anyone to come by and see," she says. "With some reasonable precautions, I think employees can be just as HIPAA-compliant working from home as they are in the workplace."

The printing issue is an example of how employees can be tripped up by the peculiarities of working at home, says **Elizabeth Litten**, JD, partner and HIPAA privacy and security officer with Fox Rothschild in Princeton, NJ. "I know of a physician who was staying at her parents' house and had to submit a lab report. She did it from her own laptop just as a quick way to transmit it. Unbeknownst to her, it also printed to the printer in her old bedroom," Litten says. "She didn't realize that for a long time. That PHI was sitting there for her parents and anyone else who happened to be there to see it. There are more opportunities for inadvertent breaches when you're working from home, even if you're trying to do it properly, because someone can just walk by and see what's on your screen or overhear what you're talking about."

Implementing good tools for remote access and ensuring verification of the user are the keys to HIPAA compliance at home, says **Matthew R. Fisher**, JD, partner with Mirick O'Connell in Worcester, MA.

"To some degree, the HIPAA considerations when having a workforce operating from their homes as opposed to the office do not introduce new concepts. The basics of ensuring that workstations and network access remain secure should be paramount," he says. "On the whole, the policies should focus on maintaining the integrity of the system and keeping data as secure as possible. For example, allowing remote access to the entire system with no more than a username and password would not be advisable. Instead, some form of multifactor authentication or other mechanisms for vetting a request for access should be implemented."

On top of system-based tools, sending reminders to individuals working remotely of how to secure work areas and data can be beneficial, he says. Reminders can take the form of teachable moments or short pieces on how to apply office-based procedures to a home environment.

IT staff will play a large role in ensuring HIPAA compliance for

remote employees, says **Timothy E. Monaghan**, JD, partner with Shutts & Bowen in West Palm Beach, FL. He says the question should be: Are our communications with employees working from home protected to the same degree as communications between our employees when working from our facilities and offices?

If the issue is communication between the healthcare entity and persons not on its payroll (such as outside counsel or consultants), the security issue is not new to COVID-19. Perhaps COVID-19 is causing the entity to review security issues in general, Monaghan offers. If this is the case, the pandemic may be uncovering issues that have been present for some time. If so, the entity would be justified in asking outside parties with whom it conducts business to demonstrate compliance with privacy and security regulations.

Another solution is to ensure sensitive information is not shared with outside parties who may not need it for their work.

"If I anticipate receiving PHI from a client, I make sure that I have a HIPAA-compliant Business Associate Agreement in place before I receive the PHI. I work with our IT folks to arrange for secure transmission and storage," Monaghan says. "Most of the time, however, I can do my work without personally identifying information. I simply advise the client to exclude that information from any communications with me."

As always, organizations should be careful to ensure PHI is shared on a "need to know" basis. This is true whether the person receiving it is working in the office or at home, Monaghan says.

"A number of HIPAA requirements have been waived. I believe this is in general recognition of the fact that we are in extraordinary times. It is more important now to keep healthcare organizations running as smoothly as possible and to simply make sure we save lives," Monaghan says. "It probably is not reasonable to expect the same level of security at home right now, but ... we should make sure that our pre-COVID practices were in order and that exceptions to full compliance are reasonable under the circumstances. In other words, we can't assume that all transgressions will be forgiven because we are in this crisis."

Covered entities should ensure HIPAA compliance the same way they did pre-pandemic: by analyzing the risks and adopting safeguards that minimize those risks, says **Jeffrey Drummond**, JD, an attorney with Jackson Walker in Dallas. There were many healthcare providers and other health industry businesses that already worked remotely or allowed employees to telecommute while maintaining HIPAA compliance.

While each business will face its own peculiar issues, some risks expected in a work-from-home situation include data transmission security, data storage security, and person/entity/device authentication, Drummond notes. However, there are readily available safeguards for each new risk.

"It's always a good idea to limit employee access to information needed for the job. Given the potential increased risk of working from home, covered entities and business associates should readdress employee access and limit wherever possible," he says. "However, a healthcare provider should not impose any data access limitations that will impact the quality of care."

HIPAA always requires taking reasonable steps to ensure the security of protected health information. Changes in work environment do not change the expected level of security, Drummond says. What is reasonable in an emergency situation may be unreasonable in a time of calm and normalcy.

"The question in current COVID-affected times is what level of security may be reasonably obtained, given the current situation? A VPN is not as secure as a closed-access system. In that respect, working from home is going to have a lower level of security," Drummond says. "However, during a time of government-mandated work-from-home orders, that 'lower' level of security might be just as reasonable — HIPAA-compliant — as the higher level during non-pandemic times."

New approaches leveraging machine learning-based data governance enable institutions to continually monitor their data, receive notifications when a compliance risk emerges, and automate its remediation, according to **Alok Tayi**, vice president of life sciences at Egnyte, a company in Mountain View, CA, that provides data security services

"Among our customers, the key risks that have emerged involve training, data exposure, and moving data between applications. To enable learning, we have seen many companies implement distributed training tools and screen sharing to share best practices," he says. "Two [tactics] to tackle data exposure are to centralize data in what is called a 'single source of truth' and apply machine learning to see when sensitive data is exposed. Native integrations between your data repository and applications facilitate a single area of control."

Considering the dynamic effect of COVID-19, transmitting data to employees working at home may be the wrong framework, Tayi says. Instead, it may be appropriate to maintain

a central, unified database to which access is provisioned. This approach facilitates a strong security envelope around the data, but affords seamless access if permitted.

"It is possible for data to be as secure in a work-from-home model as in an office-driven one. Doing so requires the proper technologies be implemented to ensure safe and secure access," Tayi says. "Approaches like machine learning-based data governance, centralized repository models, and single sign-on enable personnel and patients to have comfort and confidence around the security of their data."

Many HIPAA threats come down to inappropriate access to patient data outside the intended context. This fundamental risk to PHI data is no different in a remote work environment than in a physical office, says **Paul Trulove**, chief product officer with SailPoint, a company based in Austin, TX, that provides data security services.

"Healthcare employees should be following the same IT security best practices as they would in the office to minimize the risk of a potential data breach," he says. "Healthcare organizations can enhance their ability to protect PHI in a remote working environment by focusing on two key areas. First, ensure workers accessing PHI are connecting to a secure network when they access internal systems that have patient data. Second, make sure they are not transmitting PHI to personal devices or personal email accounts."

Employees should use corporate-owned devices and apps sanctioned only by IT, Trulove says. "Identity management is still a critical business essential as healthcare organizations continue to operate out of the home by following the same identity governance standards. To do this, they need to continually review who has access to what, and deprovision that access if it is no longer appropriate or when someone no longer works at the organization," he says. "This is critical now more than ever as people continue to be remote." ■

7 Steps to Better HIPAA Compliance at Home

Ensuring HIPAA compliance with employees working from home will require a systematic approach. **Robert K. Neiman**, JD, principal with Much Shelist in Chicago, offers seven steps for better compliance:

• Hold a Zoom call for all employees reminding them of the company's HIPPA policy and their obligations. Ensure the policy states employees working remotely and accessing protected health information (PHI) use company-owned, encrypted, password-protected, and VPN-equipped devices. Prohibit employees from using personal devices to store or access PHI. Direct all employees accessing PHI remotely to e-sign their understanding and agreement.

• Allow employees to access only the PHI they need to handle their job. Limit access accordingly.

• Prohibit any use of the company-owned device by any third party, including friends and family.

• Make sure employees' passwords for their company device and wireless router are sufficient. They should be long and complicated enough, using a combination of letters, numbers, and symbols, to minimize the risk of hacking.

• Limit PHI printing. If any employee must print any documents containing PHI, then require he or she shred printed documents before disposing them.

• Require employees working remotely to disconnect from the company system when their work is finished for the day.

• Prohibit employees from leaving their company device in their personal vehicles at any time to avoid the risk of device theft via a break-in. ■