HEALTHCARE RISK MANAGEMENT™

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

INSIDE

AHC Media
A RELIAS LEARNING COMPANY

JUNE 2017 Vol. 39, No. 6; p. 61-72

Patient Abandonment Can Occur Without Intent

The current healthcare arena, with a constricted provider marketplace and other challenges for patients seeking a new physician, can amplify the risk of inadvertent patient abandonment, says **Ilan Heimanson**, JD, partner with the Los Angeles-based law firm Heimanson & Wolf. He has handled cases in which patient abandonment was part of the theory of liability against the healthcare provider, and says many hinge on what the courts consider "sufficient notice" or "ample opportunity" to seek other care.

"In today's environment where you may have to pick from a list that has one or two preferred providers in your area, that can become an issue," he says.

With the uncertainty over the Affordable Care Act, Heimanson cautions that a patient's loss of insurance coverage does not lessen the obligation to ensure continuity of care. If the patient misses appointments because of inability to pay, the physician may have some obligation to follow up.

"Obviously, it's not the physician's job to chase down patients and make them come in for a visit, but if a significant prescription comes up for renewal and you haven't heard from the patient, a good practice would be to follow up," Heimanson says. "That's not going to be a standard of care, but if you have reason to believe that the patient is in jeopardy, it is always a good idea to take reasonable steps to investigate and urge the patient to seek help."

> IF THE PATIENT MISSES APPOINTMENTS BECAUSE OF INABILITY TO PAY, THE PHYSICIAN MAY HAVE SOME OBLIGATION TO FOLLOW UP.

Financial Disclosure: Author **Greg Freeman**, Editor **Jill Drachenberg**, Editor **Jonathan Springston**, 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. Physician Editor **Arnold Mackles**, MD, MBA, LHRM, discloses that he is an author and advisory board member for The Sullivan Group and that he is owner, stockholder, presenter, author, and consultant for Innovative Healthcare Compliance Group.

HEALTHCARE RISK MANAGEMENT™

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

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

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

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

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

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

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

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

Healthcare Risk Management™ is intended for risk managers, healthcare administrators, healthcare legal counsel, and physicians. This activity is valid 24 months from the date of publication.

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

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

Patient abandonment may be alleged after the physician fires the patient and there is no continuity of care, Heimanson says. The physician may be well within his or her rights to fire the patient, he says, but how that process is handled and documented can determine whether the physician could be held liable for patient abandonment.

Heimanson recently represented a patient who became verbally combative with his psychiatrist and was subsequently fired. The patient, who was not well enough to follow through with obtaining the proper medications from another physician, experienced mood swings that resulted in suicide.

"The pattern we see in these cases is similar to that," he says. "What you want to see on the defendant physician's side is that there was every possible effort to ensure continuity of care, and to ensure that there is a transfer of knowledge between care providers so that you don't have a patient end up with no care at all."

Avoiding Firing Patient If Possible

Firing a patient should be the last alternative when dealing with a difficult doctor/patient relationship, says **Jose I. Almeida**, MD, a vascular surgeon in Miami. He recalls firing only one patient in 20 years. Even when the physician is completely in the right, firing a patient puts him or her on thin ice right away.

"It's usually a case of communication, with you thinking you said one thing and the patient taking it another way," he says. "When these things go sideways, its usually because the patient felt wronged by the doctor, and then when the relationship ends the patient is primed to take issue with anything that might be construed as the doctor not upholding his obligation to the patient's well-being. They have legal options — and these days, they can really trash a doctor's reputation online."

Documentation will be critical, but not just at the end of the relationship, Almeida notes. Physicians should routinely make note of a patient's difficult attitude, unhappiness with the physician or staff, and similar issues because that history may be important later if the relationship is terminated.

Even the most difficult patients cannot be fired in the middle of a serious illness or episode, he says.

"That cannot even be perceived, the idea that you abandoned someone in the middle of an illness. That is a perception that can be hard to explain to others," Almeida says. "No matter how strained the

EXECUTIVE SUMMARY

A charge of patient abandonment can occur even when the provider had no intent. Physicians should be reminded of how this serious issue can manifest.

- Uncertainty over insurance coverage under the Affordable Care Act could increase the risk.
- Transferring knowledge about the patient is crucial.
- Be liberal in defining what is sufficient notice for termination of a relationship.

relationship, if there is an acute process going on, the doctor has to carry it through until the patient is stable. At that point, you can have that conversation about terminating the relationship, and it should be documented in the termination letter that the patient is now stable and care can be transferred to another physician."

Almeida notes that the loss of insurance coverage cannot interfere with the obligation to care for a patient in an acute episode.

"If they've lost their insurance in that postoperative period, you better follow them through it for free," he says. "That's an ethical obligation before it has anything to do with legal risk."

With a seriously ill or fragile patient, the physician may want to contact other professionals to try to arrange a transfer of care, Almeida says.

"That can help ensure that continuity of care, but it also can get tricky because it can be perceived as dumping, and that can lead to strains in the referral process," he says.

Professional groups recommend that the patient be provided a list of doctors and encouraged to contact them about a potential relationship. The physician also may contact the local medical board to ask for assistance in finding the patient a new doctor.

"If it's during a hospitalization, the physician should contact risk management right away, particularly if it is an acute situation or a potentially violent patient," he says.

Transfer Knowledge of Patient

Physicians sometimes focus exclusively on notifying the patient to seek other care, overlooking the need to transfer knowledge to the next caregiver, Heimanson says. This requires a follow-up system that checks on whether the patient has obtained a new physician and notification that the medical record is available for transfer.

Heimanson offers the following advice to minimize the risk of a patient abandonment charge:

• Provide the patient with written notice of termination of services by a certain date (at least 60 days in the future), and strongly advise him or her to seek another care provider.

• Ensure that the patient chart is up to date, in order, and available for the patient to pick up. Or, offer for it to be sent to the substitute provider, upon confirmation by the patient. It would be good to create a short narrative "discharge note" that outlines the patient's history, current diagnoses and conditions, and medical therapies in order to bring the new provider up to date quickly.

• If the patient is dependent on medications being prescribed by the departing care provider for health maintenance, it is crucial not to discontinue the prescription until a substitute provider has been identified and has taken over the care of the patient. If, after 30 days, the patient has not informed the care provider of the identity of the substitute provider, send a follow-up letter and/or email advising the patient that he or she must do so by a certain date.

• Develop a system that tracks these patient notifications and ensures that they were received by the patient. ■

SOURCE

- Ilan Heimanson, JD, Partner, Heimanson & Wolf, Los Angeles. Telephone: (310) 446-1522. Email: iheimanson@hwllplaw.com.

False Claims Case Alleging Forgery, Destroyed Email Moves Forward

A long-running False Claims Act lawsuit against Bon Secours New York Health System and its affiliates is moving forward in U.S. District Court for the Southern District of New York, after physicians came forward to attest that someone forged their signatures on documents required for billing. The case also may offer lessons for risk managers on preservation of email and other electronic data.

The case centers on allegations that a compliance officer was fired for trying to address healthcare fraud, and that the employer then destroyed email from her account and the accounts of a dozen more employees to hide wrongdoing.

United States of America et al. v. Bon Secours New York Health System, Inc., et al was filed by June Raffington, a masters-level nurse, who was then vice president of home care services for the Schervier Long Term Home Health Care Program in Bronx and Westchester, NY, where

she was responsible for upholding regulatory compliance and managing staff to ensure that quality standards were met. During her tenure from 2008 to 2009, she learned of forgeries of healthcare documents by company employees that violated federal and state laws, says **Jennifer Siegel**, JD, senior litigation counsel with the law firm of Sanford Heisler Sharp in New York City, and one of the attorneys representing the plaintiff.

Whistleblower Terminated from Job

Headquartered in Marriottsville, MD, Bon Secours is a nonprofit Catholic health system that owns, manages, and/or joint ventures 18 acute-care hospitals, a psychiatric hospital, five nursing care facilities, five assisted living facilities, and 15 home care and hospice programs. Bon Secours owns and operates Bon Secours New York, which operated the Schervier Long Term Home Health Care Program until its closure in 2015. Bon Secours did not respond to a request for comment.

Raffington alleges she was fired in October 2009, only a year after taking the position, for her attempts to address the company's fraudulent activities. She claims that she warned Bon Secours leaders about fraudulent billing practices for months. "Shortly before her termination, she clashed with senior leadership over the propriety of defendants' preparations for a Medicaid audit," according to her claims in court documents. "Defendants officially terminated Ms. Raffington, via letter, on October 9, 2009, four days after they sent her home to 'rest' and instructed her not to return to work."

Doctors Cite Forgery

The case has been in litigation for eight years and in recent developments, three physicians and a former staff member at Bon Secours filed declarations testifying that the agency's employees, including a former vice president, forged physicians' signatures on medical orders for patients. These forged signatures allowed the companies to fraudulently bill Medicare or Medicaid for home healthcare services, according to the lawsuit. *(See the story on page 65 for more details on the allegations.)*

The new declarations strengthen the plaintiff's case, Siegel says, because they support allegations in the lawsuit from a Bon Secours employee that a senior vice president forged doctors' signatures and ordered him to do the same.

"Doctors have now come forward filing statements attesting to the fact that their signatures were, in fact, forged. One doctor testified that her signature was forged for several years after moving from New York to Florida and was no longer seeing any patients in New York," Siegel says. "This speaks to the seriousness of the allegations in this case and the need for health administrators to timely and thoroughly investigate all allegations of fraud."

Spoliation Alleged

Following the physicians' declarations, Siegel's firm asked Judge Gabriel W. Gorenstein to sanction the Bon Secours defendants for destroying electronically stored information (ESI), including the email accounts of Raffington and 13 other individuals that may contain damning information about the companies' violations of federal and state healthcare billing laws.

The defendants waited more than six months to inform the plaintiff that disaster recovery tapes exist and can be restored for the 14 missing email accounts, according to the brief filed by firm partner **Ross Brooks**, JD.

"Defendants destroyed Raffington's email account and hard drive, as well as those of other key witnesses, including the vice president accused of ordering forgeries of physicians' signatures, and the junior staff member, whom defendants admit they fired because of allegations that he carried out such forgeries," Brooks says. "These actions satisfy the legal criteria for the court to sanction defendants for the destruction of evidence or failure to properly preserve evidence in anticipation of litigation. What they did is indefensible."

The letter to Judge Gorenstein

EXECUTIVE SUMMARY

A False Claims Act case is continuing against Bon Secours New York Health System. The plaintiff says she was fired for trying to address fraudulent billing.

- Physicians have come forward to say their signatures were forged.
- Bon Secours acknowledges destroying emails and other electronic data related to the case.
- A judge has ordered the health system to restore the data from backup tapes and provide it to the plaintiff.

asserts the defendants acted with a culpable state of mind in deleting emails relevant to Raffington's claims that should have been preserved so that they may be used in this action, committing "spoliation" of evidence in legal parlance.

The letter asks Judge Gorenstein to order the defendants to restore all requested email disaster recovery tapes at their expense and to reimburse Raffington for all fees and costs associated with investigating the spoliation and filing of the related motions. The plaintiff also requested a delay in the discovery deadline pending the defendants' production of additional documents.

"Risk managers should take all allegations of fraud seriously and investigate them thoroughly, and in good faith, at the time they are brought forward," Siegel says. "The lesson also is to preserve evidence when you reasonably expect litigation. We feel confident that the judge will rule that the defendants had an obligation to preserve all evidence in this case." ■

SOURCES

- **Ross Brooks**, JD, Partner, Sanford Heisler Sharp, New York City. Telephone: (646) 402-5668. Email: rbrooks@sanfordheisler.com.
- **Jennifer Siegel**, JD, Senior Litigation Counsel, Sanford Heisler Sharp, New York City. Telephone: (646) 402-5660. Email: jsiegel@sanfordheisler.com.

Health System Agrees to Restore Deleted Data In False Claims Act Lawsuit

In the case of *United States of America et al. v. Bon Secours New York Health System, Inc., et al,* a former compliance officer claims she was fired for trying to address healthcare fraud. These details are drawn from the lawsuit and other court documents.

The plaintiff, June Raffington, makes the following four primary allegations:

- Defendants forged doctors' signatures on some patients' plans of care that are required to support all invoices for service delivery. Other patients' cases never had plans of care completed, but invoices were nevertheless submitted for services.
- Defendants improperly billed Medicaid for services that should have been billed to Medicare, in the case of patients who had health insurance through both federal programs.
- Defendants billed New York Medicaid for services without obtaining the necessary approvals from local county departments of social services.
- Defendants retaliated against the plaintiff by firing her for complaining about and attempting to correct these fraudulent practices.

THE COMPANY ALSO STATED THAT IT DESTROYED DATA FROM THE EMAIL ACCOUNTS OF RAFFINGTON AND OTHER KEY WITNESSES, BUT SAID THE DATA CAN BE RESTORED.

Raffington filed a False Claims Act lawsuit against Bon Secours approximately one year after she was terminated. In May 2016, a U.S. District Court judge denied a motion by Bon Secours to dismiss the suit, saying Raffington had detailed the allegations in sufficient detail to proceed. In August 2016, the plaintiff requested electronically stored information (ESI) from the accounts of 27 witnesses from Bon Secours, which agreed to produce the emails and other data.

Three weeks before the initial discovery deadline, on Oct. 24, 2016, Bon Secours notified Raffington that email and other data from 14 of the 27 accounts had been destroyed. The company refused to provide information on whether the data existed on backup tapes. The plaintiff claims Bon Secours also failed to turn over a paid claims history, making it impossible for her to obtain an expert analysis that would support her claims.

On Dec. 21, 2016, a judge ordered Bon Secours to provide information about backup tapes and the paid claims history, and in February 2017, Bon Secours acknowledged that backup tapes exist. The company also stated that it destroyed data from the email accounts of Raffington and other key witnesses, but it said the data can be restored. ■

Peer-to-peer Review Would Bring Serious Risks

Peer-to-peer hospital reviews have been proposed as a way to gauge quality and compliance without waiting for the hassle and the potential ramifications of an accreditation survey, but risk managers should carefully consider the potential problems that could arise. Liability issues could make it difficult to implement such a plan.

Risk managers would be responsible for studying federal and state statutes and regulations, as well as good business practices, before consenting to such a plan, says **R. Stephen Trosty**, JD, MHA, ARM, CPHRM, president of Risk Management Consulting in Haslett, MI, and a past president of the American Society for Healthcare Risk Management (ASHRM) in Chicago. The concept may offer many potential benefits that would encourage hospital leaders to get on board with what seems like an innovative approach, he says, but it is up to risk managers to assess the downside.

Originating with the nuclear power industry, peer-to-peer reviews have been suggested for hospitals recently by some leaders in healthcare quality and safety, including a *Wall Street Journal* blog by **Peter Pronovost**, MD, PhD, John Hopkins Medicine senior vice president and director of the Johns Hopkins Armstrong Institute for Patient Safety and Quality.

"In peer-to-peer, a team of reviewers — executives, managers, front line clinicians, researchers, and others — visit another hospital for a structured, confidential, and non-punitive review of its safety and quality efforts. While it would be foolhardy to show your flaws to regulators, in peer-to-peer assessments it is encouraged," Pronovost wrote. "The goal is to create an environment of learning, not judging, for both sides. The organization being reviewed discusses its weaknesses, while highlighting its successes, which can then be shared more broadly."

True peer-to-peer reviews on a hospitalwide basis apparently have not been performed yet by any facilities, but The Johns Hopkins Hospital used a limited peer-to-peer approach when it brought in a team from Massachusetts General Hospital for a review of catheter-related bloodstream infections in ICUs and sent its own team to review the work in Boston. *(Pronovost's blog is available online at: http://on.wsj.com/2oNDYBb.)*

Trosty says hospitalwide peer-to-peer reviews are worth considering even though the execution could be challenging. Failure to thoroughly consider the legal issues could turn a well-meaning quality improvement initiative into a serious liability for the hospital.

"I do have to say that, conceptually, I like this idea and can see where there might be some real benefits. It is the sort of peer review that often can do a lot of good, but also present a variety of actual and potential problems that should be addressed and resolved prior to any agreement being entered into," he says. "It should be the role of the risk manager to help identify and research these issues and concerns, and then provide a response to hospital administration."

HIPAA compliance is one of the first hurdles. A peer-to-peer review mostly likely would involve the review of clinical or other information that contains patient-specific data, so one must decide if HIPAA would preclude this type of examination since it clearly would not be for a clinical purpose or a need-to-know basis.

"The question is whether or not this would or could fall under the exception for recognized internal peer review activities and assessments by JCAHO [The Joint Commission] and Medicare, as well as sharing information with insurance companies," Trosty says. "While we could presume this issue was evaluated and answered in the positive by Johns Hopkins and Massachusetts General before they did the peer-to-peer hospital review, I would want to do my own evaluation and talk with our hospital attorney before making a decision."

The same would apply to the issue of confidentiality and privacy from a state law perspective, he says. Risk managers must determine if it is a violation of patient confidentiality

EXECUTIVE SUMMARY

Peer-to-peer hospital reviews could help improve quality, but the idea carries some risks. Confidentiality and discoverability are key concerns.

- Hospital professionals would visit other facilities to assess quality and compliance.
- The resulting report would be confidential and nonbinding.
- Legal issues could hamper the startup of such an arrangement.

and privacy to allow a review of clinical and peer review records that might contain patient-specific information.

"Then there is the issue of potential discoverability of whatever information is shared with the team from the other hospital, especially as it relates to problems or concerns had by the hospital. Could the members of the other hospital be compelled to provide information in a medical malpractice action about what they might have learned is a self-identified problem by the hospital and it relates to the injury or claim that is the basis of the malpractice action?" Trosty asks. "Would this information be protected from discovery by the laws of the particular state as it relates to protections for peer review information?"

The potential discoverability might be affected by who requests the peer-to-peer hospital review, Trosty says. Should it be requested by the hospital attorney to try to get it protected as part of attorney-client work product? This likely would be state-specific, dependent on whether this activity and resulting report would be included in this specific protection.

There is a potential antitrust issue, especially as it relates to the hospital with whom you enter into the review agreement, Trosty says.

"Is it a potential competitor that might be interested in purchasing your hospital? Is it part of a hospital system, or even a larger hospital in another community or state that might be looking to expand into your area through acquisitions?" he says. "Some of these issues should be researched both in terms of the specific hospital with whom you might want to agree to do the services, as well as the antitrust laws that apply to your particular situation."

Risk managers also should investigate whether these activities would comply with what is set forth in the medical staff bylaws, and if not, if any amendments or additions might be required or appropriate, Trosty says. It would be important to have the medical staff on board so that they do not put up roadblocks out of concern with the use of possible results from the review, he says.

Particularly with physicians, it would have to be understood that the review itself would be nonpunitive, unlike an accreditation or compliance survey, but that the hospital would take corrective action when appropriate, Trosty says. Otherwise, the peer-to-peer review could reveal significant malfeasance or poor performance and be unable to address it. This should be allowed and provided for in the bylaws, he says.

One of the biggest concerns would be ensuring that whatever negative or potentially negative information is uncovered during the review will be kept strictly confidential by the other hospital and its personnel, Trosty says.

"It must be clearly and emphatically understood that no information obtained during the review can be shared with any other entity, organization, or individual without the written consent of the hospital being reviewed. There has to exist this trust if the review is to be effective and fair," Trosty says. "I think it is important that this be understood by all concerned and involved parties, although it will not likely be the responsibility of the risk manager to do this. However, it should be made certain that all involved persons are aware of this." ■

SOURCE

- **R. Stephen Trosty**, JD, MHA, CPHRM, President, Risk Management Consulting, Haslett, MI. Telephone: (517) 449-1285. Email: strosty@comcast.net.

Man-in-middle Attacks Pose Threat in Healthcare

The Department of Health and Human Services Office for Civil Rights (OCR) is warning healthcare providers about the risks from "man-in-the-middle" (MITM) hacking, in which someone hijacks communications between two parties and alters or copies the data without either party knowing. In addition to theft of data, MITM attacks can be used to insert malicious code or alter sensitive information like patient records.

Unfortunately, MITM attacks sometimes are made possible by a strategy intended to improve data security, OCR says. Healthcare providers, like many other organizations, implemented end-to-end connection security on their internet transactions using Secure Hypertext Transport Protocol, known as HTTPS, including software designed to detect malware over an HTTPS connection. This "HTTPS inspection" process intercepts the HTTPS network traffic and decrypts it, reviews it, then re-encrypts it before delivering the data.

This requires the installation of trusted certificates on client devices so the HTTPS inspection can be

performed without presenting warnings.

"However, this process may leave organizations using HTTPS interception products vulnerable because the organizations can no longer verify web servers' certificates, view the protocols and ciphers that an HTTPS interception product negotiates with web servers, and, most importantly, independently validate the security of the end-to-end connection," OCR explains.

Organizations using this process can validate only the connection between themselves and the interception product, not between themselves and the server.

"This is problematic, because many HTTPS interception products do not properly verify the certificate chain before re-encrypting and forwarding information to the organizations, which leaves the connection vulnerable to a malicious MITM attack," the OCR report says. *(The full OCR report, including resources for addressing the problem, is available online at: http://bit.ly/2pd2yjJ.)*

Threat to HIPAA Compliance

OCR advises healthcare providers verify their HTTPS interception product properly validates certificate chains and passes any warnings or errors to the client.

MITM attacks differ from other types of hacking because the threat occurs in the middle of an otherwise secure connection between two parties, says **Lauren M. Ramos**, JD, an attorney with McGuire Woods in Richmond, VA. The hacker effectively takes over the communication process and can intercept data, either copying it or altering it, before it is sent along to the recipient, she says.

"This can affect different industries, but in the healthcare community this is a threat to protected health information under HIPAA," Ramos says. "Once hackers intercept the information in this way and unencrypt it, they can either use it to harm the subject of the information or they might not be interested in the communication itself. Their real interest may be in using this communication as a vehicle for sending malicious code, getting it into the healthcare provider's system through this message that will pass through the security settings without a problem."

MITM attacks pose a substantial risk of HIPAA breaches, Ramos says. The OCR warning is the latest indication that the office is focusing more on the security of data in motion rather than just protecting stored data from theft or loss, she notes.

"We get focused a lot on administrative and physical safeguards because they are more intuitive and easier to grasp, particularly when it is something concrete like a laptop with PHI or a server that has to be protected," she says. "OCR is emphasizing that, while that kind of protection is essential, there is a growing threat of cyberattacks that require more technical safeguards for protecting PHI in transit. It is clear that OCR has its eye on this, and an organization's risk analysis will be under the microscope."

Risk managers may want to confirm that the organization's data security adequately addresses this type of risk, Ramos suggests. Healthcare leaders have become more adept with understanding the security necessary to prevent data theft, but may still find it difficult to understand the technical aspects of MITM attacks and how to prevent them, she says.

"When it comes to cybersecurity threats of this type, knowledge can be lacking just because it is so complex and not something that is easily grasped by someone outside of the IT department," she says. "Whether you do it with someone in-house who is very knowledgeable and can keep up with these developments, or you use an outside vendor, this is something that should be addressed before you realize it's too late. This is not something that providers are thinking about on a day-to-day basis, so it's important to make a point of assessing your vulnerability and acting proactively." ■

EXECUTIVE SUMMARY

Protected health information can be compromised by attacks on the data while it is in transit from one point to another. This is a security threat that can be underestimated by healthcare providers.

- The hijacked data may be copied or altered.
- A common security measure actually can make the attacks possible.
- Hackers can introduce malicious code with this method.

SOURCE

- **Lauren M. Ramos**, JD, McGuire Woods, Richmond, VA. Telephone: (804) 775-1168. Email: lramos@mcguirewoods.com.

Good Relations with Marketing Can Benefit Risk Management

Risk managers should open lines of communication with the marketing department to ensure HIPAA compliance and other benefits, suggests a vendor who has seen how a poor working relationship can result in problems.

There can be a disconnect between the two departments at some hospitals, says **James Chisum**, vice president of Miller Geer & Associates, a marketing firm in Los Alamitos, CA. His company regularly works with hospitals and most frequently addresses HIPAA compliance when patient testimonials will be used in marketing campaigns. The patients must sign consent forms, which will vary according to whether the patient will appear on camera, will be paid, and other considerations, he notes.

That usually means working with the hospital's risk management department to ensure all the bases are covered, but can be difficult in some cases, Chisum says.

"Being able to run something by risk management, without there being some automatic aversion to what marketing wants to do, is a positive thing. There can sometimes be some bristling from risk when marketing says they want to do this and need to be sure they're not overstepping," he says. "The better functioning hospitals have a really good line of communication between the two and understand each other's goals. Risk doesn't immediately try to put the hammer down on what marketing wants to do just because it involves patients or some theoretical risk."

> "THE BETTER FUNCTIONING HOSPITALS HAVE A REALLY GOOD LINE OF COMMUNICATION BETWEEN THE TWO AND UNDERSTAND EACH OTHER'S GOALS."

Chisum acknowledges that risk managers have a responsibility to say no to marketing when necessary, but he cautions that being too strict and reflexive can have the unintended effect of making marketers reluctant to bring ideas to the table. Still feeling the need to get their own jobs done, they may bypass risk management and hope for the best, he says.

"Nobody wants to go to someone who says no to everything all the time, so you develop a more constructive relationship when you explain what your concerns are with marketing's idea and work together on a solution that meets their goals and still keeps you in compliance," he says. "I know risk managers typically wear a lot of hats and they don't want to take on marketing as another responsibility, but keeping an open line of communication is better in the end than just saying no and avoiding it altogether."

Anticipate Media Events

Marketing campaigns are not the only way in which marketing and the hospital's communications department intersect with HIPAA compliance, Chisum notes. There also are sentinel events, high-profile incidents in the community, and other situations in which the media seeks information on patients. In those cases, the hospital often works with an outside marketing firm to manage communications and preserve its public image.

"When that happens, you want there to be an amicable relationship between risk management and marketing so that you have an open line of communication," Chisum says. "Risk might know a year in advance that the department of health is going to issue a penalty related to a patient's care, and

EXECUTIVE SUMMARY

A good working relationship with the marketing department can benefit risk management. Avoid the temptation to say no too quickly to marketing suggestions.

- Marketing campaigns often need oversight for HIPAA compliance.
- An unwelcoming attitude can lead marketers to take compliance risks.
- Work proactively with marketing on upcoming newsworthy events.

they should notify marketing well in advance of any public disclosure. That helps the marketing department put the best foot forward, but also helps avoid any inadvertent disclosures of protected information."

Working together in advance of media inquiries also helps avoid the kind of "no comment" reaction that might be well intended because of HIPAA but actually looks bad in the media, Chisum notes. Even if the information cannot be disclosed, advance notice might help the marketing department craft a more artful response.

"We've worked with less sophisticated hospitals where risk was operating in its own silo, reporting to the CEO or the C-suite and not communicating much with anyone else, and communications was working in its own silo," he says. "Risk may have known that something bad was going to hit the news eventually, but instead of providing time for communications to prepare a response, it hits them out of the blue and they have to scramble for the right response. If risk works with them ahead of time, they can help drive the communication department's response in a way that will make them more comfortable as well." ■

SOURCE

- James Chisum, JD, Vice President, Miller Geer & Associates, Los Alamitos, CA. Telephone: (562) 493-6023. Email: jamesc@millergeer.com.

California Hospital Workers Can Waive Required Meal Period

Hospital employees in California are now allowed to waive one of their required meal periods, but risk managers should obtain proper consent before employees skip any meals.

The Fourth Appellate District reversed its previous February 2015 decision in *Gerrard v. Orange Coast Memorial Medical Center* and ruled that healthcare employees may waive one of their two required meal periods on shifts longer than eight hours, even if the shift exceeds 12 hours, says **Diane Marie O'Malley**, JD, partner with Hanson Bridgett in San Francisco.

On Feb. 10, 2015, the court invalidated the portion of California Industrial Welfare Commission (IWC) Wage Order No. 5 that permitted non-exempt healthcare employees to waive a second meal period for shifts longer than 12 hours. The decision was retroactive for four years, so California healthcare employers faced substantial liability for allowing employees to waive their rights to meals.

Then in October 2015, Gov. Jerry Brown signed SB 327 into law, allowing healthcare employees to voluntarily waive their right to one of their two meal periods in shifts of 12 hours or more. The appellate court revisited its decision in light of the new law, and reversed its earlier ruling.

> "ONCE YOU HAVE THAT WAIVER, HOWEVER, DON'T FORGET THAT THE EMPLOYEE IS FREE TO REVOKE IT WITH JUST ONE DAY'S NOTICE."

"For years, healthcare employees working directly in patient care were waiving one of their meal periods, even when working more than 12 hours, mostly because if they were already working long hours they didn't want to be there any longer. They preferred to just eat at their desk or whatever and get out sooner," she explains. "Then there was a class action lawsuit in which the employees said it was in violation of the California labor code."

Though the most recent decision is good news, hospitals in California still should tread carefully when allowing employees to waive their right to a required meal period, O'Malley says.

"This clarifies that eligible employees can continue what they were doing before this issue came up, which is waiving a meal period they're entitled to," O'Malley says. "But for the employer to be safe, there should be a written agreement that's signed by the employee and the employer. Once you have that waiver, however, don't forget that the employee is free to revoke it with just one day's notice." ■

SOURCE

- Diane Marie O'Malley, JD, Partner, Hanson Bridgett, San Francisco. Telephone: (415) 995-5045. Email: domalley@hansonbridgett.com.

$33 Million Verdict After Doctor Took Stockbroker Call During Delivery

A Florida jury issued a $33.8 million medical malpractice award to the family of a baby who suffered permanent brain damage during a delivery in which the obstetrician paused to take an eight-minute phone call from his stockbroker and tried to cover his tracks by falsifying the mother's medical record.

After the verdict, the Florida Department of Health reopened its investigation into the physician, according to a report by *The Miami Herald*. *(The report is available online at: http://hrld.us/2q4pfa7.)*

Nineteen-year-old Marla Dixon delivered her child at North Shore Medical Center in Miami, and a jury found that her doctor made a series of errors leading to the child's permanent disability. Ata Atogho, MD, ordered nurses to restart a drug to strengthen contractions, failed to perform a cesarean section, and walked away from the patient for long periods, according to the newspaper report. One absence was for an eight-minute phone call with his stockbroker, the jury determined.

Dixon testified that the doctor blamed her child's injuries on her for not pushing hard enough. The doctor falsified the mother's medical record with a note that made it appear she had refused a cesarean section, according to the testimony of the nurse in charge of delivery. The mother maintains Atogho never apologized for his actions.

The U.S. Attorney's Office represented Atogho because he worked for the federally funded Jessie Trice Community Health Center at the time. The U.S. government will pay the $33.8 million fine.

In addition to the Dixon case, Atogho delivered two babies the same year who were permanently brain damaged, and a third who was disabled for life. All the mothers received care at Jessie Trice, which serves many of Miami's low-income and uninsured residents, the newspaper reports. ■

HHS Offers Guide on Measuring Compliance Effectiveness

The Department of Health and Human Services Office of Inspector General (OIG) is offering a guide to measuring the effectiveness of a hospital or health system's compliance program.

The guide, titled "Measuring Compliance Program Effectiveness: A Resource Guide," was developed by a group of compliance professionals and applies to a wide range of organizations with diverse size, operational complexity, industry sectors, resources, and compliance programs, OIG reports. The goal is to provide "as many ideas as possible, to be broad enough to help any type of organization, and let the organization choose which ones best suit its needs."

However, OIG emphasizes that the guide is not intended to be a best practice, template, or checklist. The purpose of the resource guide is to document the idea-generating discussion by the roundtable participants, but given OIG's participation, there is the potential for it to be incorrectly construed as the agency's recommendations or even requirements, OIG notes.

The guide is available online at: http://bit.ly/2nFBFCZ. ■

CME/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.

COMING IN FUTURE MONTHS

- Treating the electronic health record as medical record
- Fire Safety: What to look for and improve
- Best career path for risk managers
- How much should the board know?

HEALTHCARE RISK MANAGEMENT™

CME/CE INSTRUCTIONS

To earn credit for this activity, please follow these instructions:
1. Read and study the activity, using the provided references for further research.

2. Log on to AHCMedia.com to take a post-test. Go to "My Account" to view your available CE activities. First-time users must register on the site using the subscriber number printed on their mailing label, invoice, or renewal notice.

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

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

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

CME/CE QUESTIONS

1. **What does Ilan Heimanson, JD, partner with the Los Angeles-based law firm Heimanson & Wolf, say is sometimes overlooked when terminating a relationship with a patient?**

   a. Transfer of knowledge of care to the next caregiver
   b. Billing records
   c. HIPAA release forms
   d. Digital imaging

2. **When does Jose I. Almeida, MD, a vascular surgeon in Miami, say a physician should never terminate the relationship with a patient?**

   a. In the first 60 days
   b. When the patient has expressed dissatisfaction with the doctor's care
   c. In the middle of a serious illness or episode
   d. After a relationship of one year or more

3. **In the case of *United States of America et al. v. Bon Secours New York Health System, Inc., et al*, what does the plaintiff allege?**

   a. She was fired for trying to address healthcare fraud.
   b. She was fired for refusing to address what the hospital thought was fraud, but she disagreed.
   c. She was unfairly denied a promotion because of her experience at another facility.
   d. She was unfairly denied a promotion because of her education.

4. **What is a "man-in-the-middle" attack?**

   a. Someone hijacks communications between two parties and alters or copies the data without either party knowing.
   b. A vendor steals protected health information.
   c. A staff member at the hospital unlawfully obtains protected data.
   d. An outside hacker seizes important data and demands a ransom.

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

Defendants Prevail on Failed Kidney Transplant Appeal

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

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

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

News: A woman received a kidney transplant after it was determined she suffered from fatal end-stage renal disease. The patient's brother provided the transplanted kidney. Following the surgery, the kidney failed, and ensuing complications resulted in a removal of the transplanted kidney. After receiving an adverse decision in a medical review process, the patient and her brother filed suit for medical malpractice. Discovery revealed the plaintiffs did not intend to use an expert witness to determine the standard of care or otherwise testify. The defendants filed a motion for summary judgment, which the trial court granted.

In the resulting appeal, the appellate court determined that expert witness testimony was necessary to establish the plaintiff's claims. As a result, the trial court's grant of the defendants' motion for summary judgment was upheld.

Background: In 2009, a woman presented to a hospital, where it was determined she was suffering from end-stage renal disease and placed on peritoneal dialysis. The patient needed a kidney transplant. She was briefed on the kidney transplant process, and consented to be evaluated for a transplant. It was determined that her brother would be her kidney donor.

The patient underwent surgery on May 11, 2010. Several days later, the patient's transplanted kidney failed because she suffered from a twisted kidney, a condition associated with functional problems in the way urine drains to the bladder, and with vesicoureteral reflux — when urine flows backward through the urinary system. The patient underwent additional medical procedures to correct the problem, but these also failed, resulting in removal of the kidney.

DISCOVERY REVEALED THE PLAINTIFFS DID NOT INTEND TO USE AN EXPERT WITNESS TO DETERMINE THE STANDARD OF CARE OR OTHERWISE TESTIFY.

Shortly after the patient was released from the hospital, she and her brother initiated a medical review panel process. The medical review panel found in favor of the healthcare providers, determining they did not breach the applicable standard of care. The plaintiffs proceeded to file a medical malpractice lawsuit, alleging negligence and failure to obtain informed consent. While many defendants were named in the seven different complaints filed, all were dismissed save for the initial surgeon (for causing the problem), the corrective surgeon (for failing to correct it), and the hospital (liable under applicable law for the actions of the surgeons).

Two years after filing the lawsuit, and six years from the initiation of the medical review panel, the remaining defendants filed motions for summary judgment, alleging that the plaintiffs lacked the necessary expert testimony to support the petition's claims. After a hearing on the motions for summary judgment, the trial court ruled in favor of the defendants.

The plaintiffs then filed an appeal on the grounds that granting the motion for summary judgment was improper

because the medical review panel did not conform with Louisiana's Medical Malpractice Act and was inadmissible, the defendants failed to obtain the appellant's informed consent, and expert witness testimony was unnecessary for some of the allegations. Before the hearing on the appeal, the patient died, and her brother proceeded on behalf of himself and the patient's estate.

In its review of the case, the Louisiana Court of Appeal first noted the fact that at the trial level, the plaintiffs failed to timely file their opposition to the motion for summary judgment and filed the opposition with inadmissible attachments. The court then limited the scope of issues on appeal to whether the plaintiffs could prove their allegations of medical malpractice without the use of expert witness testimony.

In determining whether the trial court's ruling on the summary judgment was in error, the court of appeal noted that only in cases where negligence is so obvious that a layperson can infer negligence without the guidance of expert testimony can a plaintiff prevail without the use of an expert. The court then stated that in this case, involving a kidney transplant and other related procedures, a layperson could not ascertain the appropriate standard of care. The court addressed the lack of informed consent as well, and noted that the establishment of such a claim in Louisiana requires the identification of the risk and the probability of the risk occurring, which in turn require expert testimony to prove. The court of appeal thus affirmed the defendants' motion for summary judgment.

What this means to you: This case clearly illustrates that expert testimony is critical in medical malpractice cases. Because of the plaintiffs' failure to secure an expert on the standard of care, the issue of obtaining informed consent was not even reached by the court. This was important for the defense because, notwithstanding plaintiffs' contention that the physicians did not inform them properly and obtain their consent, the plaintiffs signed nine consent forms. However, the appellate court noted it appeared the patient's consent forms were signed by a family member on her behalf. If no oral information was given to the patient before the surgery commenced, there may have been an issue with the signer's authority to sign on the patient's behalf.

To avoid problematic informed consent allegations, medical professionals must ensure that individuals who sign on behalf of others are authorized to do so. A frequently used mechanism for verifying that authority is an executed and notarized power of attorney. More generally, physicians are required to provide complete information to patients about any procedure the patient requires so that the patient can decide whether to proceed. This information must include the risks that might occur, the benefits of undergoing the procedure, alternative treatments available, and expected recovery time. Informed of this, the patient can consent or refuse to proceed. Documentation by the physician in the patient's medical record is mandatory, including the patient's understanding of the information.

Furthermore, the informed consent cannot be provided by a nurse or any other non-independently licensed individual and must be provided to the patient unless there is a documented reason why the patient is mentally unable to receive, process, understand, and conclude from the information whether to have the procedure. Providing informed consent to a family member, friend, or other representative of the patient is not acceptable if the patient has the capacity to understand it. Often, the opinion of a psychiatrist is required before informed consent can be provided to someone other than the patient. It is helpful if patients without capacity have advance directives, developed when the patient had capacity, to guide others about the patient's choices of a decision-maker and his or her wishes for life-sustaining measures should the patient's condition deteriorate. Physicians often misstep during the informed consent process and later find themselves in legal battles over failures of critical parts of the process.

Finally, this case shows the importance of understanding the applicable standard of care in a case. The court rejected the plaintiffs' contention that a layperson could ascertain the standard of care for a kidney transplant without the aid of an expert witness. The court of appeal gave the following nonexhaustive list of circumstances in which the standard of care is readily determined by a layperson: fracturing a leg during examination, amputating the wrong arm, dropping a knife, scalpel, or acid on a patient, or leaving a sponge in a patient's body. This list makes it clear that complex surgeries generally will not fall into the category of cases in which expert testimony on the standard of care is unnecessary. In any medical malpractice matter involving a complex surgery, it is critically important for both sides to line up supporting expert witnesses at the outset of the case. ■

REFERENCE

Decided on April 5, 2017, in Court of Appeal of Louisiana, Fourth Circuit, Case No. 2016–CA–0873.

Unnecessary Surgery Results in $625,000 Verdict

News: In 2013, a woman underwent surgery to remove a mass in her abdomen. The operating physician reviewed reports from several other physicians, who allegedly determined the patient had a mass the size of a potato. When the surgeon began the procedure to remove the mass, he found nothing to remove and consulted with a general surgeon, who confirmed there was no mass. Because of the surgery, the patient suffered internal damage that required her fallopian tube to be removed, preventing her from bearing children.

The patient and her husband sued the operating physician as well as several other persons. After a battle of the experts, the eight-member jury returned a $625,000 verdict in favor of the plaintiffs to compensate for lost wages, medical expenses, loss of consortium, and disfigurement.

Background: On May 10, 2013, an obstetrician-gynecologist at a Pennsylvania health center performed an unnecessary exploratory laparotomy on a patient that caused scarring and adhesive disease. Prior to the procedure, a radiologist at a separate hospital read a transvaginal ultrasound taken of the patient on April 23, 2013, as revealing a 6 cm mass, but the ultrasound scan was, in fact, normal. Another radiologist allegedly read a May 8, 2013, CT scan of the patient's pelvis as suspicious for a solid mass, but in a different part of the patient's body. Again, the scan was normal, and no solid mass existed. The two radiologists were allegedly employees and agents of the hospital and the OB/GYN was an employee of the health center.

In deciding to proceed with the surgery, the OB/GYN relied on the reports of the two radiologists, which contradicted his own findings of a normal pelvic and rectal exam, the report of a GI specialist who conducted a rectal exam, and a normal colonoscopy. The OB/GYN also ignored the recommendations of the two radiologists to order a CT scan with rectal contrast, and an MRI. Furthermore, the two radiologists' reports noted the mass in different areas of the patient's body; thus, the physician concluded it was a "mobile mass."

THE TWO RADIOLOGISTS' REPORTS NOTED THE MASS IN DIFFERENT AREAS OF THE PATIENT'S BODY; THUS, THE PHYSICIAN CONCLUDED IT WAS A "MOBILE MASS."

The OB/GYN contended he discussed the surgery with a general surgeon to confirm he should remove the mass via a mini-laparotomy, but refer the patient to the general surgeon if the mass was mesenteric. The general surgeon alleged that he was not consulted before the surgery and that if he did discuss the surgery with the OB/GYN beforehand, he would have examined the patient and reviewed the medical studies. In fact, the general surgeon alleged that the first time he encountered the case was when the obstetrician called him into the operating room because he could not find any mass in the patient's open abdomen.

On Nov. 14, 2014, the patient filed a medical malpractice claim in the U.S. District Court for the Eastern District of Pennsylvania. In February 2016, three years after the surgery and four months after the complaint was filed, a physician performed an exploratory laparoscopy to evaluate the integrity of the patient's left fallopian tube. He found significant pelvic adhesive disease with occlusion of the left fallopian tube. The physician cut the adhesions and removed the patient's fallopian tube.

In a second amended complaint on July 25, 2016, the patient and her husband alleged medical malpractice and loss of consortium claims against the OB/GYN and the health center at which he was employed, and the radiologists and their employing hospital. The plaintiffs alleged, inter alia, failure to properly diagnose, monitor, and treat the patient, failure to perform exploratory surgery laparoscopically, and failure to properly read the April 23, 2013, transvaginal ultrasound and the May 8, 2013, CT scan of the pelvis.

On Feb. 15, 2017, the hospital was dismissed by stipulation of the parties, and the case proceeded to trial against the physicians and health center. At trial, the plaintiff's gynecology expert offered the opinion that the surgery and loss of female anatomy was a direct result of the OB/GYN's unnecessary surgery. The defendant radiologists' expert in radiology opined that because they expressed uncertainty, requested further studies, and did not make the decision to perform surgery, they met the standard of care. The OB/

GYN's expert opined that he was justified in relying on the reports of the radiologists and physical exam by the patient's family physician.

After the five-day trial, the eight-member jury found the OB/GYN 100% liable. On March 22, 2017, an amended judgment was entered in accordance with the verdict in favor of the patient for $625,000.

What this means to you: First and foremost, this case presents the issue of consultation of and respect for other physicians. The two radiologists offered their reports, but were hesitant about the existence of a mass. The OB/GYN disregarded recommendations by the two radiologists to perform further tests to ensure the mass existed. At trial, the radiologists' expert did not opine that they read their respective tests accurately. Rather, the expert opined that the uncertainty they expressed and the fact that they were not responsible for the decision to perform the surgery were sufficient to satisfy the applicable standard of care. If the OB/GYN had given more deference to the radiologists' concerns about the existence of a mass and investigated further, it is possible that this case would have been prevented altogether.

This case also shows the importance of conducting thorough pre-surgery exams to ensure patients do not have pre-existing conditions that may complicate the procedure and result in otherwise avoidable liability for the healthcare provider. Here, the OB/GYN had access to reports from three different physicians, but it is unclear whether he had access to the patient's full medical record. At trial, the defense argued that the adhesions were caused by chlamydia the patient contracted in 2006. However, when the OB/GYN conducted the exploratory laparotomy, he took note in his operative report that he checked the patient's uterus, ovaries, and fallopian tubes, and found them to be normal and did not find signs of adhesions or endometriosis. This report created a strong causation argument for the plaintiffs: When the patient underwent surgery in 2013, there were no adhesions, but in 2016, there were adhesions. If the chlamydia did cause the adhesive disease, the OB/GYN failed to observe and note any signs when operating.

The discovery rule — which generally tolls or suspends the running of the statute of limitations — became relevant to this case when the amended complaint was filed. The first complaint did not allege the loss of female anatomy since the fallopian tube had not yet been removed. Under the circumstances, the subsequent discovery of the latent harm that required removing the fallopian tube did not preclude the patient from amending her complaint and adding the claim against the OB/GYN, because the plaintiff had no reason to previously suspect the existence of this issue. Note that, though typically delay in litigation benefits the defense, a countervailing consideration is that sometimes delay results in a plaintiff discovering additional harm. Although subsequent and excusable discovery of an injury may not preclude later litigation, an early settlement may induce the plaintiff to voluntarily waive all remaining claims known and unknown, and preclude later litigation.

Finally, while the defense did not raise the issue in this case, informed consent again could have been used here to show that the patient knew of the risks of the exploratory laparotomy and chose to undergo the surgery. Transparency with patients is key to preventing suits because it puts more responsibility on the patients and makes them feel like the physician has their best interests in mind — an important factor in determining whether an adverse medical result becomes a lawsuit at all.

That said, there are limitations to this idea. It would be extremely unfair to burden the patient entirely with the decision to proceed when facts are ambiguous. If the surgeon is uncertain, would the patient have a better understanding? This is highly doubtful. Clearly, a reasonable physician facing a similar situation should follow the standard of care required by repeating both the ultrasound and CT scan, obtaining an MRI if indicated by the new studies, and, if any ambiguity remained, consulting an expert in the field, be it a general surgeon or more senior OB/GYN before surgery, and asking that surgeon to assist with the surgery or be readily available. The female reproductive organs are continually active, with cysts forming both ovarian, in utero, and endometrium. It is imperative that as much accurate information as possible be available before any invasive procedure takes place. If it is determined that a mass does exist but the nature of the mass is difficult to establish, a physician also might consider repeating tests and waiting several weeks to establish the continued existence of the mass, thus avoiding invasive procedures and preventing scar tissue formation, which leads to adhesions and further internal complications. ■

REFERENCE

Decided on March 17, 2017, in U.S. District Court for the Eastern District of Pennsylvania, Case No. 14-cv-06674.

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

What You Think You Know About HIPAA Might Be Wrong

Healthcare organizations take HIPAA seriously and typically devote substantial resources to education and monitoring, but misconceptions about the privacy law still can trip up the best efforts.

One of the most common misconceptions concerns when a healthcare provider needs a business associate agreement (BAA) with a vendor, says **Ira Parghi**, JD, an attorney with Ropes & Gray in San Francisco.

HIPAA requires covered entities, including hospitals, to put BAAs in place with their vendors in certain circumstances, but there is a fair amount of confusion as to what those circumstances are, Parghi says.

HIPAA requires a BAA if the vendor receives protected health information (PHI) from the covered entity to provide services to or on behalf of the covered entity, Parghi explains. The decision to frame a certain vendor relationship as a business associate relationship has important implications, she notes.

"The BAA, or other accompanying contract, must set forth a number of required elements, with the result that a BA relationship entails certain concrete contractual obligations. HIPAA also imposes certain duties, such as the requirement to have privacy and security policies, on BAs as well as covered entities," Parghi says. "And from an enforcement perspective, growing attention is being placed on BA relationships, with regulators often asking, for instance, how the covered entity has managed a particular BA relationship, or whether and how the BA has implemented its own training and policy requirements."

Both parties in a BA relationship must be prepared, organizationally and financially, to "manage to" the agreement, Parghi says, meaning they must organize their operations in such a way as to uphold their various contractual and HIPAA obligations, some of which can be quite resource-intensive.

> BOTH PARTIES MUST ORGANIZE THEIR OPERATIONS IN SUCH A WAY AS TO UPHOLD THEIR VARIOUS CONTRACTUAL AND HIPAA OBLIGATIONS, SOME OF WHICH CAN BE QUITE RESOURCE-INTENSIVE.

Some covered entities have erred on the side of requiring BAAs with all their vendors as a matter of course, without considering the specific nature of a particular vendor relationship. Consequently, such covered entities require BAAs from vendors that do not receive PHI from the covered entity (and are, therefore, not BAs), or who only come into occasional incidental contact with PHI while performing their work (and, therefore, fall under the HIPAA exception for incidental disclosures).

"We have seen healthcare institutions try to enter into BAAs with elevator servicing companies, cafeteria management companies, and the like, and in general, such relationships are not going to constitute BA relationships for HIPAA purposes," Parghi says. "On the other side of the spectrum, some covered entities do not require their vendors to sign BAAs when they should. For instance, vendors of electronic medical record platforms, and the companies that respond to patient requests for record copies on behalf of hospitals, are almost certainly going to be BAs."

Outside attorneys and other experts, collection

companies, photocopy companies, and practice support vendors may be BAs, depending on, for instance, the type of information disclosed to them, Parghi says. An attorney who assists on a corporate deal without ever seeing the names or any other information about patients likely is not a BA, but an attorney who provides advice on potential HIPAA breaches and reviews specific privacy incidents while conducting that work likely is.

A company that only photocopies financial records that have no patient information may not be a BA, but a company that photocopies clinical information likely is, she explains.

"Related to this, some covered entities have been known to sign BAAs provided to them by their vendors without carefully reviewing them, or to vary the terms of their own forms of a BAA too readily when asked to by a vendor, without weighing the request carefully. These approaches, too, can create risk," she says.

HIPAA also sets out certain exceptions to the BA requirement, Parghi notes. For example, exceptions may apply to vendors that are serving as "conduits" for PHI only, vendors who only come into incidental contact with PHI and take certain required precautions, and vendors who are healthcare providers to the patients in question. These also require fact-specific analyses, rather than assuming the answer.

"Whether a particular HIPAA exception to the BA requirement applies in a certain case, and what operational and other steps should be taken to ensure that that exception applies coherently, are questions that covered entities and vendors are urged to discuss with their legal advisors," Parghi says.

Legal advice also is a good idea when considering whether to carry out risk analyses under attorney privilege, Parghi says. There may be pros and cons to both approaches.

The popularity of concierge medicine, or the overall effort to make physicians more accessible to patients, increases the risk of HIPAA breaches via telephone, says **Andy Altorfer**, CEO of CirrusMD, a healthcare technology company in Denver. The physician may provide his or her cellphone number to the patient, giving little thought to the security of exchanging PHI in that way, he says.

"Sometimes, they have the patient sign a waiver, but that does not absolve your data security concerns," Altorfer says. "Texts are stored on non-secure telecom servers, with identifiable patient information and PHI. You don't have BAAs with those entities and they have no documented security or auditing, so typical phone texts will always be a fundamental HIPAA security breach."

HIPAA Security Rule compliance remains challenging for some healthcare providers, Parghi says. They often misunderstand the nature and scope of their obligations under the Security Rule, she says.

The Security Rule is organized into three sections that discuss the technical, administrative, and physical safeguards that a covered entity must carry out with respect to electronic PHI, Parghi explains. Each category of safeguards enumerates specific implementation standards, some of which are "required" and others of which are "addressable." All the implementation standards are "technology neutral," meaning that they do not mandate the use of specific technologies, she says.

"One common point of confusion for covered entities arises with the interpretation of 'addressable' implementation standards. Addressable standards, contrary to common perception, are not optional. They must be implemented if it is reasonable and appropriate to implement them," she explains. "And if the decision is made to not implement them, the decision should be appropriately documented. Unfortunately, some covered entities have misunderstood this requirement, and hence not approached these decisions and their documentation appropriately."

In addition, Parghi says healthcare providers sometimes fail to appreciate that many of the obligations arising under the Security Rule are ongoing obligations, not "one-time only" technological fixes. For instance, risk analyses under the Security Rule are supposed to be updated annually and also in the event of certain material changes, such as a change to a hospital's electronic medical record system.

"Regulators have sometimes asked for annual risk analyses from the years before, during, and after a breach, and providers who have not updated those risk analyses annually have found themselves penalized," she says. "Likewise, ePHI access and use is required to be monitored on an ongoing basis, and regulators may request evidence that, during a certain time frame, such access and use was properly monitored, and instances of potentially improper access or use appropriately investigated."

Misconceptions also can arise over the potential scope of Security Rule compliance investigations, which often are much more expansive in scope than one might expect, she says. Regulator inquiries may not just focus on the specific requirements in the Security Rule that are pertinent

to a particular privacy or security incident, more broadly assessing general compliance with Security Rule requirements. For instance, regulators may ask for copies of annually updated risk analyses, various policies and procedures, information about access controls, breach assessments, security logs, and the like, Parghi says.

"A healthcare provider undergoing a Security Rule investigation may find that, once the hood of the car is opened, much of it will be inspected," Parghi says.

Security Rule compliance is most effective when a range of stakeholders are included, Parghi says. Successfully implementing the various requirements under the Security Rule is an ongoing, and resource-intensive, process, she notes.

"In our experience, the healthcare providers who are most successful have generally been able to bring together important stakeholders from seemingly disparate functions in the organization, such as information security, compliance, information technology, and clinical risk management, and encouraged them to work cooperatively," Parghi says. "Too often, the only personnel who understand HIPAA are the ones who lack technological training, and the only personnel with technological expertise are not well-trained on HIPAA's Security Rule requirements."

Healthcare providers also can misunderstand what is allowed when providing patient information to clinicians, says **Heather Delgado**, JD, partner with the firm of Barnes & Thornburg in Chicago. Physicians sometimes request information on a patient and are told that it cannot be provided because of HIPAA restrictions, and Delgado says that almost always is not correct.

"There is a treatment exception in HIPAA that allows clinicians to share information about patients, but we still see clinicians refused and there is no reason for it," Delgado says. "When they block that access, that's actually when they're in violation of HIPAA because HIPAA fully states that you can share PHI for treatment purposes. This can come up often with specialty providers trying to get information on a patient, and it can be detrimental to the patient's care and safety."

Delgado notes that healthcare providers often assess the success of their HIPAA training by how well employees know when and how to protect PHI, without also assessing their understanding of when not to block access. This can lead to employees choosing to err on the side of caution and say no to data access when they are doubtful or just don't know if it is allowed, she says.

"A lot of the HIPAA mistakes you see could be prevented from the outset if there was proper training," Delgado says. ■

SOURCES

- Andy Altorfer, CEO, CirrusMD, Denver. Telephone: (720) 593-9549. Email: contact@cirrusmd.com.
- Heather Delgado, JD, Partner, Barnes & Thornburg, Chicago. Telephone: (312) 338-5905. Email: heather.delgado@btlaw.com.
- Ira Parghi, JD, Ropes & Gray, San Francisco. Telephone: (415) 315-1285. Email: ira.parghi@ropesgray.com.

HIPAA Not Just About High-tech Security

One of the most common mistakes is to perceive HIPAA compliance as solely or predominately a technology problem, says **Michael R. Overly**, JD, partner and privacy and data security lawyer at the law firm of Foley & Lardner in Los Angeles. He has heard administrators and other healthcare professionals say that their organization is HIPAA-compliant because the IT department has everything locked down with all the right software, encryption, and other technological solutions, as if that is enough.

"That is a problem, because if you look at the statistics in just the last year, two-thirds arose not from a technology failure, but rather human error," Overly says. "It is very hard to get people to start thinking about how HIPAA compliance is their responsibility and doesn't fall entirely on the technology side."

While some investment in technology is necessary, Overly cautions against the easy assumption that spending a lot on a software solution makes you compliant. That same $100,000 might have a bigger effect if it is spent on employee education, he says.

The goal should be to make information security a personal issue for individuals in healthcare, Overly says, but he admits that can be a hard sell. One way to get the message across is to show how understanding HIPAA security can help them in their personal lives, he suggests. He used this approach at a grand rounds presentation at a hospital, finding the audience much more receptive than they usually are to lectures on HIPAA compliance.

"You want to show them that if they grasp the key elements of HIPAA compliance, they can also benefit from that knowledge to protect their family photographs stored in the cloud, their tax records stored on their home computers, and their email accounts when they are under attack," Overly says. "When you explain to physicians that they might go home that night and find all their years of family photographs gone forever, you get them leaning forward. Then they will listen to how the same techniques that they can use to secure their data at home can also be effective in complying with HIPAA at work."

Another misconception is that HIPAA is all about confidentiality and security, Overly says. The component often overlooked is integrity — the validity and accuracy of the protected data, he says. This is where hackers are starting to focus more attention, potentially with ransomware attacks.

"We've seen ransomware attacks in which hackers take away our access to data and make you pay to get it back, but I worry that we're going to start seeing attacks on integrity of data, which could be devastating in healthcare," Overly says. "It's one thing if the hacker just has your data, and it's something else if that hacker says your data is going to be destroyed or hopelessly compromised. With people's healthcare information, that can have very serious consequences."

Overly also cautions that the backup tapes providers depend on to preserve PHI also could be exploited by hackers. People often assume that they have little to worry about if their data is backed up, but Overly says it is crucial to assure that those backups are not infected with malware or have security vulnerabilities.

"If you're subject to an attack, the first inclination is to just restore your data from a backup tape. What people don't realize is that hackers know that and sometimes will use malware that makes its way to your backups and then sits dormant for months until you try to use that tape," he says. "You would think that by now healthcare providers would be aware of that, but we're seeing that is not the case."

Few healthcare providers also have a plan for stopping a malware attack from multiplying, Overly says. If one clerk in accounting accidentally clicks an email link and infects that department's computer system, there should be an immediate response once that is detected, he says. An immediate and wide-reaching alert to every other department and all staff should notify them about that particular email or threat so they can avoid more infections, he says.

"An infection in the accounting department doesn't have to spread and affect every other part of the system. People assume that once it's in one time, that malware is spreading through the whole organization and that's not necessarily so," Overly says. "But if different departments are attacked, you can have multiple points of access for the malware and that makes the attack much more serious."

Another misconception is that HIPAA requires encryption of ePHI, says **Peter Tippett**, MD, PhD, chairman of DataMotion, a company in Florham Park, NJ, that provides security and compliance assistance to healthcare facilities. Although encryption is well-advised for any ePHI in transit or stored on mobile devices, it is not actually required by HIPAA, he says.

You could theoretically say you've performed a risk assessment and determined that the encryption is unnecessary, Tippett says.

"Encryption is all about making the data useless after a theft, so for your big mainframe computers, for instance, you might say that you have all kinds of extensive security with cameras, and cages, and locks, and so forth that makes the threat of theft very low with that hardware," Tippett says. "So, it would be reasonable in that instance to say you're not going to encrypt that stored data. I've seen that work a number of times, but it's not something most organizations would imagine doing."

Organizations also can emphasize technological security so much that the low-tech ways to violate HIPAA are overlooked, says **Dennis Deruelle**, MD, FHM, national medical director for acute services with IPC Healthcare/TeamHealth, a company providing healthcare professional staff and integrated care providers in Tampa, FL.

"We teach people about the risk from texting, hackers, and lost laptops, but you also have the low-tech breach where someone walks into a room and starts talking about something sensitive with the family or others present," he says. "That even happened to my wife. Her surgeon walked into the room and said, 'You have a little nodule on your lung,' in front of eight people." ■

SOURCES

- Dennis Deruelle, MD, FHM, National Medical Director, Acute Services, IPC Healthcare/TeamHealth, Tampa, FL.
- Michael R. Overly, JD, Partner, Foley & Lardner, Los Angeles. Telephone: (213) 972-4533. Email: moverly@foley.com.
- Peter Tippett, MD, PhD, Chairman, DataMotion, Florham Park, NJ. Telephone: (800) 672-7233. Email: info@datamotion.com.