

the REPORTER

OPHTHALMOLOGY 2011

Failure to evaluate patient

by Tanya Babitch, senior risk management representative

This closed claim study is based on an actual malpractice claim from Texas Medical Liability Trust. This case illustrates how action or inaction on the part of physicians led to allegations of professional liability, and how risk management techniques may have either prevented the outcome or increased the physicians' defensibility. The ultimate goal in presenting this case is to help physicians practice safe medicine. An attempt has been made to make the material more difficult to identify. If you recognize your own claim, please be assured it is presented solely to emphasize the issues of the case.

Presentation

A 72-year-old man was evaluated by Ophthalmologist A on several occasions. The patient had cataracts, with best corrected visual acuity of 20/25 in the right eye and 20/40 in the left eye. Ophthalmologist A recommended surgery to remove the cataract from the left eye.

After discussing the risk and benefits of surgery, Ophthalmologist A performed an uncomplicated cataract surgery with intraocular lens implant on the patient's left eye. The patient was prescribed both pre- and post-operative antibiotic and steroidal eye drops.

Ophthalmologist A saw the patient the next day for a post-operative examination. The patient reported a slight headache and that his vision was still "a little cloudy." Visual acuity was documented as 20/60 in the left eye. Ophthalmologist A noted 2+ inflammation in the left eye, but he did not find this to be concerning. The patient was told that it would take time for his vision to improve.

Physician action

Saturday morning — two days after the surgery — the patient called and spoke with Ophthalmologist B, who was taking call for Ophthalmologist A. The patient claimed that he reported floaters, decreased vision, and the sensation of looking through a lace overlay in the left eye. Ophthalmologist B recalled that the patient did

not complain of any pain, which would be expected if there were an infection. Ophthalmologist B claimed that he offered to see the patient in the office that day and told him to call back if his condition changed. Ophthalmologist B did not document this conversation in the patient's medical record.

The patient recalled the conversation differently. He claimed that Ophthalmologist B simply instructed him to continue with his medications, but did not offer an appointment that day. The patient called again on Sunday morning, complaining that his vision in the left eye had worsened. The patient claimed that he was again instructed by Ophthalmologist B to continue with the medications and see Ophthalmologist A on Monday.

Ophthalmologist B reported that when the answering service notified him of the call, the service indicated that the patient complained of pain. However, when actually speaking to the patient, Ophthalmologist B reported the patient denied pain and did not report worsening vision. The patient was most concerned about running out of ketorolac trometamol eye drops. Ophthalmologist B said that he explained to the patient that if he was not experiencing any pain there was no need to prescribe any more drops. He advised the patient to discuss this with Ophthalmologist A on Monday. Ophthalmologist B recalled offering the patient the option to be seen that day, and he denied that the patient told him that his vision had deteriorated

continued on page 2

continued from page 1

substantially. This second conversation with the patient was not documented.

The patient returned to Ophthalmologist A on Monday, reporting to the nurse that he had received “no help” from Ophthalmologist B over the weekend. Of note, Ophthalmologist A’s documentation of this visit included that the patient denied pain over the weekend and discussed running out of eye drops. Ophthalmologist A diagnosed the patient with endophthalmitis and referred him to a retinal specialist for a same-day appointment.

The retinal specialist saw the patient that day and confirmed the diagnosis of endophthalmitis. The retinal specialist took the patient to surgery that evening and performed a vitrectomy with injection of intraocular antibiotics. The retinal specialist confirmed that there was a hypopyon involving the anterior segment of the eye, which is an indication of an acute bacterial infection.

Cultures of the ocular fluids obtained during surgery were initially negative. However, final cultures grew *Staphylococcus* coagulase-negative, but the lab noted “from broth only” and “possible skin flora contaminant.” After the vitrectomy, the patient’s vision could be refracted to 20/60, but he had ongoing difficulty with recurrent inflammation and retinal detachments. He required three additional surgeries. The patient ultimately lost the use of his left eye and has only light perception vision.

Allegations

A lawsuit was filed against Ophthalmologist B, alleging failure to evaluate the patient in person when his symptoms required it. The patient alleged that he reported symptoms to Ophthalmologist B that justified immediate evaluation and treatment. Had he been evaluated in person, the eye infection would have been treated sooner, preventing his loss of vision. Ophthalmologist A was not sued.

Legal implications

Consultants who reviewed this case felt that the delay in evaluation and treatment of the patient over the weekend negatively affected the patient’s outcome. Had the vitrectomy with the injection of intraocular antibiotics been performed sooner, the patient may have had an improved result. However, the consultants also stated that if the actual complaints reported to the on-call ophthalmologist did not indicate any signs of infection (pain, worsened vision) it would offer some defense to the physician. Unfortunately, these phone calls were not documented, and there was no way to determine what had been said.

The cause of the patient’s endophthalmitis was unknown. The ocular fluid culture obtained during the vitrectomy was initially negative. However, the final result was not entirely conclusive, and there were questions about possible contamination. Consultants stated that negative cultures did not rule out an infection, particularly since the patient had already been given antibiotics.

Though the retinal specialist documented clear signs of bacterial infection, one consultant argued that the negative cultures could

have indicated an inflammatory process as opposed to an infective process. However, the retinal specialist stated that there was an infection present. Consultants believed it was likely that the patient’s infection occurred at the time of surgery; therefore, it existed before the patient’s involvement with Ophthalmologist B. However, it was the consensus among the consultants that had the patient been evaluated by Ophthalmologist B over the weekend, the infection would have been identified and treated more promptly.

Disposition

This case was taken to trial. Based on the jury questions that were submitted to the judge during their deliberations, it was apparent that the jurors were having difficulty deciding the case because of the lack of documentation of the conversations between the patient and Ophthalmologist B. This case was settled during jury deliberation at trial.

Risk management considerations

In this case, the lack of documentation clearly compromised the physician’s defense. Had Ophthalmologist B documented what the patient told him — that there was no pain or significant worsening of vision — his actions would have been more defensible.

Documentation of telephone conversations with patients, including after-hours and weekend calls, is prudent risk management. Although this documentation can be challenging, it is in both the physician’s and the patient’s best interest to document the details of any calls. Phone call documentation should include not only what the patient reported, but the physician’s specific response or advice.

Options for the documentation of after-hours or weekend calls include the use of dictation and pocket message pads; logging on to electronic medical records and entering a note; or review of answering service logs to prompt physician documentation. Practices have come up with many creative ways to facilitate documentation of calls. Some use answering service logs to allow staff to pull paper charts for physician documentation, or to enter “tasks” in the electronic medical record. Electronic tasks that include the patient name, time of call, and any other details supplied by the answering service, can then be sent to the physician for review and completion. Other practices have devoted phone lines that physicians can “speed dial” to dictate a quick note about the call received. Staff can then transcribe the note into the patient record the following day and distribute to the physician for review and sign-off.

Physicians are encouraged to try different methods of documentation to determine what works best for their practices. Although never easy, documentation of after-hours calls can assist subsequent providers in providing appropriate patient care, and may also be valuable in the defense of a malpractice claim or Texas Medical Board complaint.

Tanya Babitch can be reached at tanya-babitch@tmlt.org.

Highlighting HIPAA and HITECH — changes enacted to privacy rules

by the TMLT risk management department

As part of the American Recovery and Reinvestment Act of 2009, Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act. This legislation contains provisions that strengthen and expand HIPAA's privacy and security requirements and offers a number of financial incentives to promote the adoption and meaningful use of electronic medical records. It also makes significant changes to existing patient privacy laws and imposes increased civil and criminal penalties for their violation. (Civil penalties for each violation range from \$100 to a \$50,000 minimum.)¹

This article will address data breaches involving protected health information (PHI) and the new requirements for business associates. Physicians are strongly urged to review their privacy policies and procedures to assure compliance and avoid significant fines.

Background

In 1996 the U.S. Department of Health and Human Services (HHS) issued the Privacy Rule, establishing for the first time national standards for the protection of certain health information. The Privacy Rule — also known as HIPAA — was originally enacted to help employees maintain their health insurance coverage during a time of job change; to establish privacy and security rules for PHI to set standards for electronic billing of health care services; and to develop a national provider identifier system. Most physicians and medical practice staff are all too familiar with the standards related to protecting the use and disclosure of patients' PHI.

Protecting PHI

The new legislation requires physicians to review current practices related to the use and disclosure of PHI and make any necessary revisions. Prior to this legislation, a covered entity (e.g. physician's office, hospital, clinic, etc.) was only required to mitigate the effects of an unauthorized disclosure. This may or may not have included notifying the patient. Under the revised law, with few exceptions, a covered entity is required to notify a patient of an unauthorized disclosure of unsecured PHI if a significant risk of "...financial, reputational or other..." harm exists when a breach of unsecured PHI has been discovered.¹

Notification must occur without reasonable delay — no more than 60 days after the breach is discovered. Any notification to the patient must include:

- a brief description of what happened;
- the type of PHI disclosed;
- steps the patient should take to protect him or herself;
- what the covered entity is doing to investigate and mitigate the breach; and

- information concerning whom to contact for additional information.

"Notification must be in writing by mail (or by phone in urgent cases) or electronic means if the patient has consented to electronic notification. If the breach involves more than 500 patients (e.g. the loss of a laptop containing unsecured PHI), local media outlets must be notified. In addition the HHS secretary must be notified immediately for breaches involving more than 500 patients and annually for others."²

Please note that notification is only required if the breach involved unsecured PHI. HHS has issued guidance about the definition of "secured" PHI. Information is deemed secured if rendered "... unusable, unreadable, or indecipherable..." to unauthorized individuals.³

If the breach involved information that is secured, then notification is not required. This rule applies to two categories of secured PHI: electronic PHI that meets specified standards of encryption and PHI stored or recorded on media that has been destroyed. Adoption of this rule provides a significant incentive for physicians to encrypt PHI.⁴

Securing PHI involves two main components. The first involves encrypting electronic PHI by using software that renders the information unreadable until the intended recipient unlocks it (with a smart card and password). Elements that should be encrypted include:

- practice management systems;
- electronic medical records;
- documents containing PHI (e.g. claims payment appeals);
- scanned images, such as copies of remittance advices;
- e-mails containing PHI;
- PHI transmitted electronically, such as claims sent to clearinghouses; and
- PHI made available through the Internet.

The second component involves properly destroying the media on which the PHI is stored or recorded, such as shredding paper records or purging electronic information.⁵

Additional information about encryption can be found at the American Medical Association web site, <http://www.ama-assn.org/ama1/pub/upload/mm/368/hipaa-phi-encryption.pdf>

Business associates

Effective February 17, 2010, business associates are required to comply with the revised regulations, and are subject to the same requirements as covered entities for implementing administrative,

Texas Medical Liability Trust
 P.O. Box 160140
 Austin, TX 78716-0140
 800-580-8658 or 512-425-5800
 E-mail: laura-brockway@tmlt.org
www.tmlt.org

Editorial committee

Bob Fields, President and CEO
 Jill McLain, Executive Vice President, Claim Operations & Risk Management
 Don Chow, Senior Vice President, Sales & Business Development
 Dana Leidig, Vice President, Communications & Advertising
 Sue Mills, Vice President, Claim Operations

Editor

Laura Hale Brockway, ELS

Associate Editor

Louise Walling

Graphic Designer

Karen Ow

Pre-sorted Standard
 U.S. Postage
 PAID
 Permit No. 90
 Austin, Texas

the Reporter is published by Texas Medical Liability Trust as an information and educational service to TMLT policyholders. The information and opinions in this publication should not be used or referred to as primary legal sources or construed as establishing medical standards of care for the purposes of litigation, including expert testimony. The standard of care is dependent upon the particular facts and circumstances of each individual case and no generalizations can be made that would apply to all cases. The information presented should be used as a resource, selected and adapted with the advice of your attorney. It is distributed with the understanding that neither Texas Medical Liability Trust or Texas Medical Insurance Company is engaged in rendering legal services.

© Copyright 2011 TMLT

HIPAA and HITECH ... continued from page 3

physical, and technical safeguards for PHI. Business associates must also revise written policies and procedures covering these requirements, and will be subject to the same civil and criminal penalties as covered entities.

The Office for Civil Rights (OCR) is the federal agency responsible for enforcing the federal privacy rule. According to Sue McAndrew, deputy director for health information privacy for the OCR, "Business associates can be directly liable for a breach of unsecure protected health information (PHI) and could have to pay OCR directly."⁶

Both covered entities and business associates must review all relationships with contractors to assess whether business associate agreements are in place and are compliant with the new requirements.⁵

TMLT as a business associate

As a professional liability carrier, TMLT is considered a business associate of its policyholders. As such, TMLT will appropriately safeguard any protected health information it receives or creates on behalf of physicians. To assist physician practices in complying with the revised rules, TMLT has developed a new Business Associate Agreement. The revised agreements were recently mailed to all policyholders, and are also available on the TMLT website at: <http://www.tmlt.org/hipaa>.

Policyholders are urged to complete the revised agreement, and return it by fax to 512-425-5999. The form can also be mailed to TMLT Underwriting Services, PO Box 160140, Austin, TX 78716-0410. Signed agreements will remain on file in the TMLT Underwriting Services Department.

Conclusion

HIPAA rules, regulations, and standards will continue to change under the direction of the federal government. It is important that practices' policies and procedures are periodically reviewed and updated to reflect these changes. Initial training of new staff members and ongoing re-training of current staff is required under these revised regulations.

Sources

1. U.S. Department of Health and Human Services. Breach notification rule. Available at: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule>. Accessed July 20, 2010.
2. U.S. Department of Health and Human Services. Guidance to render unsecured protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Available at: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html>. Accessed July 19, 2010.
3. Sanders DL, Kern SI. What the HITECH Act means for you. *Medical Econ*. March 19, 2010.
4. Texas Medical Association. Secure patient information mitigates risk for your practice. Published July 16, 2010. Accessed July 20, 2010.
5. HealthLeaders Media. Business associates can pay directly for breaches. February 4, 2010. Available at www.healthleadersmedia.com/print/TEC-246029/Business-Associates-Can-Pay-Dire. Accessed July 19, 2010.
6. U.S. Department of Health and Human Services. HITECH Act. Available at: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coverentities/hitechact.pdf>. Accessed July 20, 2010.