

the REPORTER

ANESTHESIOLOGY 2011

Failure to monitor patient during outpatient surgery

by Shannon Quinn, 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 55-year-old woman came to a plastic surgeon to discuss cosmetic improvement of her facial features. During her appointments, the patient reported a medical history of obesity, hypertension, fibromyalgia, and lupus. Her medications included metoprolol, pregabalin, hydrochlorothiazide, and hydroxychloroquine. After two appointments, the patient and plastic surgeon decided on blepharoplasty and a facelift. The surgery was scheduled to take place in an outpatient surgery center.

The surgeon advised the patient that a pre-surgical clearance was needed. He referred the patient to a family practice physician next door to his office. After an EKG, blood work, and a chest x-ray, the patient was cleared for surgery. The family physician's report for surgical clearance did not mention the patient's obesity or any of her other pre-existing conditions as risk factors.

Physician action

The patient arrived at the outpatient surgery center for the procedure. She met with the anesthesiologist, who documented the assessment of physical status as a 2/3, based on the American Society of Anesthesiologists (ASA) physical status classification system. This meant the patient was qualified as having moderate systemic disease.¹

The patient was pre-medicated with pentazocine and naloxone 50 mg and diazepam 10 mg given orally at 7:11 a.m. She was then given 2 mg of midazolam and 2 cc of fentanyl and taken to the operating room. The patient's initial vital signs were within normal limits.

Anesthesia was induced at 7:23 a.m. After the anesthesiologist administered propofol 40 mg, the patient's blood pressure dropped to 116/50 mm Hg. Her other vital signs were normal. Next, the anesthesiologist gave a second bolus of propofol 40 mg. The patient's vital signs were recorded as BP 118/50 mm Hg; pulse rate of 66; and spontaneous respirations. Oxygen was administered via nasal cannula; however, rate of flow was not documented. The anesthesiologist administered a third bolus of propofol 20 mg. The time that each propofol dose was given was not documented.

Upon entering the operating room at 7:48 a.m., the surgeon noticed the patient's fingernail beds were blue. The anesthesiologist administered epinephrine and the surgeon began injecting local anesthetic to the patient's eyelids and chin, using 20 cc lidocaine 2% with epinephrine and 10 cc bupivacaine 0.5% with epinephrine. The patient did not register any response to the painful stimuli of the injections. The patient's blood pressure dropped to 100/40 mm Hg with a pulse rate of 56. The anesthesiologist administered .02 mg of glycopyrrolate, but the patient's pulse dropped to 30. The surgeon stopped the injections and began CPR. The anesthesiologist intubated the patient and EMS was called at 8:09 a.m.

EMS arrived at 8:31 a.m. The EMS record reported the patient's pulse rate to be 30; oxygen saturation 82%; BP 70/30 mm Hg; respirations were absent; Glasgow score of 3; and the patient's pupils were dilated and unreactive.

The patient arrived at the hospital at 8:57 a.m. Initial lab values showed a pH of 7.15; PCO₂ of 33; and PO₂ of 106. The admission record noted the patient was suffering from

continued on page 2

continued from page 1

metabolic acidosis consistent with significant lack of oxygen. CT scans showed severe swelling of the brain, consistent with anoxic encephalopathy. An MRI of the brain ruled out a stroke and a CT scan of the chest ruled out pulmonary embolism. Two consulting neurologists indicated that the patient was in a coma due to an anoxic event.

The patient, who was in a persistent vegetative state, was discharged from the hospital a month later and transferred to a nursing home. She did not regain consciousness and died in the nursing home three years after the surgery.

Allegations

A lawsuit was filed against the anesthesiologist and the plastic surgeon. The allegations included

- negligence in administering excessive anesthesia;
- failure to adequately monitor the patient;
- failure to recognize a respiratory arrest; and
- failure to timely and appropriately respond to the respiratory arrest.

Legal implications

This case presented many challenges for the defense. Multiple consultants who reviewed the case shared the opinion that due to the patient's co-morbidities, she was a poor candidate to have elective cosmetic procedures performed in an outpatient setting. The consultants agreed that her obesity made her prone to airway obstruction, and the documented ASA assessment of physical status of 2/3 did not support operating in an outpatient setting.

The consultants also agreed that excessive sedation was used. Although the anesthesiologist described the anesthetic technique as moderate sedation, it was felt that the amount of sedation given and the patient's lack of response to painful stimuli indicated that general anesthesia was instead administered. Due to this level of sedation, there was criticism that an end tidal CO₂ monitor was not used intra-operatively. It was felt that the patient's arrest and subsequent outcome was respiratory in etiology, suggestive of respiratory depression caused by medications.

There were also concerns about the lack of documentation in the anesthesia record. The level of oxygen flow through the nasal cannula, the times the drugs were administered, and proper documentation of ACLS protocol during resuscitation were not documented.

Risk management considerations

Patients who are scheduled for office-based anesthesia typically do not meet the anesthesiologist until the morning of the procedure; therefore, it is important for the anesthesiologist and the surgeon to develop policies and procedures to determine which patients are good candidates for office-based anesthesia.² ASA guidelines state "patients who by reason of pre-existing medi-

cal or other conditions may be at undue risk for complications should be referred to an appropriate facility for performance of the procedure and the administrations of anesthesia."³ The consultants in this case felt that this procedure should have been performed in a hospital setting.

The patient's pre-surgical screening was questionable because her pre-existing conditions and body mass index were not mentioned in the evaluation. The fact that the patient was cleared by a physician recommended by the plastic surgeon, rather than the physician who followed her for her pre-existing conditions, was also detrimental to the case.

The Texas Medical Board (TMB) has outlined specific rules related to office-based anesthesia services. TMB Rule Section 192.2 outlines requirements pertaining to pre-anesthesia diagnostic testing, physiologic monitoring, documentation, equipment, and policies and procedures development.⁴ It is recommended that anesthesiologists and surgeons offering office-based anesthesia services familiarize themselves with the TMB rules and review their practices to ensure they are in compliance with state regulations.

Disposition

The defense could not locate an expert who was supportive of the defendants. Based on the critical consultant reports and the significant exposure associated with three years of intensive nursing home treatment for the patient, the case was settled on behalf of the anesthesiologist.

The plastic surgeon involved in the case did not carry medical liability insurance and was forced to file for bankruptcy. Many of the surgeon's assets were seized to cover her portion of the settlement.

Sources

1. American Society of Anesthesiologists. ASA Physical Status Classification System. Available at <http://www.asahq.org/For-Members/Clinical-Information/ASA-Physical-Status-Classification-System.aspx>. Accessed June 28, 2011.
2. Twersky RS. Office Based Anesthesia: Challenges and Success. Available at http://www.csaol.cn/img/2007asa/RCL_src/204_Twersky.pdf. Accessed June 22, 2011.
3. American Society of Anesthesiologists. Guidelines for Office-Based Anesthesia. Available at <http://www.asahq.org>. Accessed June 22, 2011.
4. Texas Medical Board. Board Rules, Texas Administrative Code, Title 22, Part 9 (Section 192, 217-221). Available at http://www.tmb.state.tx.us/rules/docs/Board_Rules_Effective_05.05.2011.pdf. Accessed June 22, 2011.

Shannon Quinn can be reached at shannon-quinn@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

Charles R. Ott, Jr., 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/coveredentities/hitechact.pdf>. Accessed July 20, 2010.