

Failure to treat post-operative infection

by Shannon Quinn, associate 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 69-year-old woman was referred to an orthopedic surgeon for a defect in her Achilles tendon. She was diagnosed with a chronic rupture of the Achilles tendon. The patient was given the options of either living with the defect or undergoing reconstruction to regain strength and function. The patient chose to proceed with the reconstruction. The orthopedic surgeon — the defendant in this case — performed a repair with transfer of the flexor hallucis muscle.

The surgery was uneventful, and the patient was administered a one-time dose of vancomycin post-operatively. Vancomycin was selected because the patient was allergic to penicillin. The patient was discharged the following day with instructions to leave her foot in a splint. She was to follow up with the orthopedic surgeon within ten days.

Physician action

The patient followed up with the surgeon eight days after surgery. She was noted to have some skin irritation and some minimal drainage. Because the wound was slow to heal, the surgeon made the decision to leave the sutures in place for another week.

The patient returned a week later, and the sutures were removed. The wound was observed to have some minimal wound granulation and drainage from the incision. These observations of the wound were written in a different handwriting from the surgeon's, but were not initialed. The surgeon believed that they were in his nurse's handwriting, but he could not be sure. It was also unclear if the entry was what the patient had relayed to the nurse, or if those observations were made by the nurse herself. The patient was fitted with a splint to continue immobilization of the foot and was told to only remove the splint to bathe. She was also advised to complete wet-to-dry dressing changes, to monitor the wound for signs of infection, and to return to the office in four weeks.

Nearly one week after this office visit, the patient called the surgeon's office and received a prescription for ciprofloxacin. The only record of this encounter, which occurred five days after the patient's last visit, was the pharmacy record. There is no record of the phone call, what was discussed, or the reason for the prescription.

continued on page 2

continued from page 1

Two days later, the patient came to the surgeon's office complaining that her foot was "feeling hot" and noting a "hole" in the wound. She was not wearing her splint. The patient claimed that she was not advised to do wet-to-dry dressing changes, but instead was told by the surgeon's nurse to clean the wound with peroxide, then dress with dry gauze. The surgeon examined the wound, noted minimal cellulitis, but did not feel the area was hot. He advised to continue taking ciprofloxacin, discontinue the improper peroxide cleanings, and proceed with wet-to-dry dressing changes.

The patient called three days later, while the surgeon was on vacation, to report that the wound drainage was getting worse and now had an odor. The patient was advised to come to the office, and was seen by the surgeon's partner. This office note was incomplete, only stating: "post-op wound infection, culture taken." This second surgeon, not realizing the patient had a penicillin allergy, gave the patient a prescription for amoxicillin clavulanate. Fortunately, this mistake was caught by the pharmacy, and another antibiotic was substituted. The patient stated in her deposition that this was what made her lose confidence in the surgeon's office. She sought treatment from a wound care facility four days later. The wound care physician diagnosed her with full thickness dehiscence, necrotic subcutaneous fatty tissue, and necrotic areas of the tendon in the wound base.

Six days later after the patient's appointment with her surgeon's partner, the lab results were returned indicating *staphylococcus* and *actinomyces meyeri* infections. The patient was called and asked to come to the surgeon's office that day. She was emergently referred to a plastic surgeon, who admitted her for IV antibiotics and several debridements of the wound.

Allegations

A lawsuit was filed against the orthopedic surgeon, alleging that he failed to timely and adequately treat the patient's post-operative infection. She claimed that function of her lower leg was impaired as a result of the infection and the failed Achilles tendon graft.

The patient underwent subsequent surgeries with a plastic surgeon to remove the original tendon transfer due to necrosis of the tissue. Tissue from the patient's wrist was transplanted to the original surgical site to fill the void left by the removed tissue. The patient claimed the subsequent surgeries resulted in the loss of sensation in her fingers.

Legal implications

TMLT consultants who reviewed this case were generally supportive of the orthopedic surgeon. Infection is a known complication of Achilles tendon repair. There also appeared to be some question of patient compliance. However, all of the consultants had some concerns about the lack of adequate documentation pertaining to justification of the antibiotics chosen.

The surgeon's partner had also missed elements of the documentation, and did not provide detail about why he chose amoxicillin

clavulanate. However, the only defendant in this lawsuit was the orthopedic surgeon who performed the repair.

Disposition

This case was settled on behalf of the orthopedic surgeon.

Risk management considerations

Although infection is a known complication inherent in any surgical procedure, there were several problems with the surgeon's documentation that complicated the defense of this case.

It is recommended that all phone calls between the patient and physician be documented, particularly calls in which medical advice is given. There was no record of the patient's call that triggered a prescription for ciprofloxacin, or reason for the change in the treatment plan. Documentation of the patient's symptoms, description of the wound and any noted changes, and the physician's reasoning behind treatment not only creates a thorough chart, but in this case, it would have provided additional information to the surgeon's partner when he saw the patient.

Implementing a protocol that requires all staff making entries in the chart to initial or sign their entries will assist in identifying who made the entry in case it needs to be verified at a later date.

It is recommended that physicians have a policy and procedure manual for the practice to ensure that all personnel are operating under the same guidelines, as expected by the physician. This may include any routine instructions that are commonly given to patients, such as how to perform a wet-to-dry dressing change. It is further recommended that important instructions to the patient be developed into a handout that can be given to the patient and to document that the handout was given. Patients often get confused when instructions are given in the office, which can make compliance difficult. Should a claim occur, the printed instructions could be used as evidence to show precisely what information was given to the patient.

It is appropriate for medication allergies to be consistently and boldly documented on the front of the chart to prevent them from being overlooked when prescriptions are written. All physicians in the same practice should standardize how allergy information is displayed if they cover for one other. It was fortunate that the pharmacy caught the error before the prescription was filled; however, the error made the patient lose confidence in the practice. A patient and/or the patient's family are more likely to file a lawsuit if they perceive that the care they are receiving is substandard.

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

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.