

the REPORTER

INTERNAL MEDICINE 2011

Failure to perform a thorough exam

by Wendy Kaliszewski, 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 75-year-old man came to his internal medicine physician's office complaining of right leg weakness and swelling, phlebitis, and leg pain described by the patient as a "charley horse," as well as right foot swelling. The patient had been seeing this physician for eight years. His medical history included double hernia repair, COPD, chest pain, hypertension, hyperlipidemia, pulmonary embolism, degenerative disc disease and chronic DVT dating back eight years. Three months prior, the internal medicine physician had prescribed support stockings due to the patient's thrombophlebitis. The patient had also been treated for pneumonia a month earlier.

Physician action

At this visit, the patient's pulse was 74 and his blood pressure was 172/90 mm Hg. The patient stated that he had not taken his blood pressure medication that morning. Lab values were within normal limits.

The internal medicine physician examined the patient's leg, but did not remove the support stocking. He ordered an ultrasound duplex extremity venous bilateral scan to be performed the next morning.

At home, the patient's wife removed his stockings and noted that his ankle and foot were purple. She also noted small blood veins in a cluster under the skin, described as "worms". The patient told his wife that the internal medicine physician did not remove the stocking during his exam. The patient took an aspirin and elevated his legs.

The ultrasound duplex scan was performed the following morning. After the scan, the patient came to the physician's office complaining of severe back pain, for which he requested an injection.

While in the waiting room, the patient began gasping for air and complained of feeling faint. An office staff member tried to administer oxygen, but the tank was empty and one had to be transported from another office. The patient slumped forward and the internal medicine physician started CPR. EMS arrived and the patient was taken to the ED in full arrest. He was pronounced dead shortly after his arrival.

The physician received the results of the ultrasound duplex after the patient had been taken to the ED. The impression was chronic occlusive thrombus extending from the right common femoral vein through the popliteal vein, with collateral vessels that were not incompetent. The left leg Doppler was normal. An autopsy revealed massive pulmonary embolism with relatively recent thrombus material in both right and left pulmonary arteries and evidence of previous pulmonary emboli. Leg discoloration, a mottled mid ankle and spider veins were noted on the right.

Allegations

The patient's family filed a lawsuit against the internal medicine physician. The allegations included:

- failure to perform a proper exam of a patient "who presented with a history of blood clots in his leg, along with recent leg pain and swelling;"

continued on page 2

continued from page 1

- failure to timely diagnose the blood clot;
- failure to order a STAT diagnostic evaluation; and
- failure to timely admit the patient to the hospital for treatment.

Legal implications

The plaintiff’s expert indicated that the physician should have done a more extensive examination of the patient’s right leg to include removal of the stocking and careful inspection of the leg for redness, tenderness, swelling, increased temperature, and palpable venous cord. It was further asserted that the patient should have been hospitalized for an emergent venous Doppler scan, lung scan, and heparin therapy.

A consultant who reviewed this case for the defense stated that the physician should have questioned the patient more closely about the pain in his leg and should have removed the stocking to observe the condition of the leg. He also reported that the office records were of poor quality and did not accurately reflect the patient’s care, potentially leading to missing the significance of pleuritic chest pain and an abnormal chest x-ray approximately one month before the events. These issues initiated the litigation.

Disposition

This case was taken to trial and the jury returned a verdict in favor of the plaintiffs.

Risk management considerations

The defense consultant was critical of the documentation of the patient encounter, noting there was little useful information about the physical exam or the patient’s history. Some of the

physician’s previous notes lacked detail and thoughtfulness. A thorough physical exam and a review of the patient’s history are important diagnostic tools for physicians. This includes asking-focused questions and making close observations, including palpation and percussion of the affected area. This is especially important given the acute onset of symptoms in a patient with a complex medical history.

The documentation of the visit is equally important. The Texas Medical Board (TMB) rules state that, “Each licensed physician of the board shall maintain an adequate medical record for each patient that is complete, contemporaneous and legible.”¹ This includes documentation of all relevant history, assessment, clinical impression, plan of care, and the legible identity of the observer. A complete medical record may be the physician’s safeguard against future allegations of negligence.

It is also advisable to maintain a written emergency plan and policy. An emergency policy ensures that all staff members know what to do during an emergency. This policy should be updated annually and signed by all staff members and physicians. The policy should also include a regular check of the emergency equipment to ensure that it is functioning properly. Basic emergency equipment should include oxygen, airways, and oxygen masks.

Source

1. Texas Medical Board. Board Rules. Available at www.tmb.state.tx.us/rules/rules/bdrules.php. Accessed August 21, 2011.

Wendy Kaliszewski can be reached at wendy-kaliszewski@tmlt.org.

TrendsMD
Connecting physicians

TMLT has launched a new blog, TrendsMD. It will connect physicians and other professionals who are interested in discussing medical liability issues. A variety of physicians, attorneys, and insurance experts will contribute to TrendsMD.

We invite you to visit the site and add it to your bookmarks. Please feel free to comment on articles that interest you.

Find the site at <http://www.trendsmd.com>



Video CME when you need it!

TMLT now offers three CME videos. Completing all three can earn a 3% discount (not to exceed \$1,000) that will be applied to the next eligible policy period.

- You’re not alone: managing litigation stress
- Successfully navigating your deposition
- CMS, MAC, RAC, and MIC: what do they mean to me?

Visit <http://www.tmlt.org/services/video> now to watch these videos.

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.