

Failure to diagnose cardiac arrest

by Michele Luckie, 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 37-year-old man came to the emergency department (ED) complaining of chest pain. The pain was located in the left anterior chest region, and began 30 minutes before he arrived in the ED. The patient reported that he felt weak and sweaty.

Physician action

The patient was triaged immediately. An emergency medicine physician evaluated him and began cardiac protocol. An IV was started, and the patient was given an aspirin and sublingual nitroglycerin every 5 minutes for 15 minutes. The patient's EKG was interpreted as borderline normal with no acute ischemic changes. The chest x-ray was reported as clear. Lab work was ordered.

The patient continued to have considerable chest pain, described as non-radiating and located in the left anterior chest area. He was given 4 mg of morphine intravenously with minimal response. Approximately 40 minutes later, he was given 30 mg of Toradol intravenously. A second EKG was performed. Thirty minutes passed and the patient was still experiencing significant pain. He was given 8 mg of intravenous morphine. Shortly after receiving this dose of morphine, the patient's discomfort was greatly relieved.

The emergency medicine physician reported that the second EKG showed no changes, although the patient developed mild bradycardia. The lab work indicated normal chemistries and normal cardiac enzymes. Due to the difficulty in alleviating the chest pain, the emergency medicine physician ordered a CT of the chest to rule out a pulmonary embolism. The CT was reported as normal.

The patient was now reporting that his chest pain had improved significantly. After a discussion with the patient about obtaining a cardiac evaluation, the emergency medicine physician called a cardiologist and scheduled a stress test for the patient. Approximately 4 hours after presenting to the ED, the patient was discharged with a diagnosis of atypical chest pain. He was advised to take aspirin and to return to the hospital if the pain recurred.

Early the next morning, the patient was found gasping for breath. His wife called EMS. The paramedics documented that the patient was in asystole and apneic. He was immediately intubated, started on

continued on page 2

continued from page 1

oxygen, and given drugs to stimulate his heart. CPR was initiated. After 8 minutes, the patient regained a heartbeat and spontaneous respirations. He was transported to the hospital. Upon arrival, he was found to have had a full cardiac arrest. He was posturing and had a seizure, which suggested some hypoxic cerebral damage.

The cardiac arrest resulted in a 23-day hospital stay that included a cardiac catheterization and angioplasty with stents. The patient was sedated and remained intubated during the early part of his hospitalization.

At discharge, the patient was alert, communicative, in good spirits, and looking forward to returning to work. His discharge diagnoses included ventricular tachycardia and fibrillation; cardiac arrest; anoxic encephalopathy; and acute inferior wall myocardial infarction status post emergency angioplasty and triple stenting of the right coronary artery. The patient was released to cardiac rehab and instructed to follow up with the cardiologist and a neurologist to monitor his seizure activity. The patient eventually returned to work, but claimed he could not perform as well due to his cognitive deficits and inability to concentrate.

Legal implications

A lawsuit was filed against the emergency medicine physician. The allegations included:

Failure to order serial 12-lead EKGs; failure to seek a cardiac admission for 23-hour observation; and failure to order diagnostic testing, including serial cardiac enzymes. It was alleged that the patient would not have suffered a cardiac arrest and anoxic encephalopathy if the defendant had more thoroughly evaluated the patient.

The plaintiff's experts criticized the patient history taken by the defendant. It was "missed" that the patient smoked two packs per day for 20 years. This information was documented by subsequent health care providers. It was also alleged that the diagnostic work up fell below the standard of care. The emergency medicine physician listed myocardial ischemia or infarction as the first

differential diagnosis, but she failed to order a 6-hour troponin that would have helped rule out that diagnosis. The plaintiffs argued that a patient with severe, intermittent pain, a history of tobacco dependency, and two abnormal EKGs with dynamic changes should be considered an acute coronary patient in the absence of any other explanation for the symptoms.

Defense experts were generally supportive of the care provided by the emergency medicine physician. However, they agreed that the patient should have been admitted for observation and repeat enzymes. While defense experts were impressed that a cardiology opinion was obtained, given the patient's history of tobacco use, they felt it would have been prudent to have the cardiologist examine the patient before discharge.

Risk management considerations

Emergency medicine physicians are responsible for conducting a basic evaluation and providing a reasonable assessment of a patient's medical condition. A thorough patient history is critical to this process; perhaps even more so when a patient complains of chest pain. The fact that the patient was a long-time smoker is a key piece of information affecting treatment decisions. In this case, the patient denied smoking, but his wife stated that he was a 2.5 pack per day smoker. She stated that anyone could tell the patient smoked by standing close to him. Had the emergency physician known this, she would have admitted the patient for observation and requested a cardiac consult. This may have led to a more timely diagnosis. Using all reliable sources to gather health information — including risk factors — can affect timely treatment and improve patient outcomes.

Disposition

This case was settled on behalf of the emergency medicine physician.

Michele Luckie can be reached at michele-luckie@tmlt.org.

ARE YOU CONTRACTING AWAY YOUR RIGHT TO BE INSURED BY TMLT?

If you are thinking about becoming employed in an Accountable Care Organization (ACO) or Non-Profit Health Organization (NPHO) aka 5.01(a),

DID YOU KNOW THAT:

1. **You may not be able to keep or choose your medical liability insurance carrier.** Consequently, you may be required to put your reputation and assets in the hands of the organization's self-insured entity rather than with the proven insurance professionals at TMLT.
2. **You may lose the right to withhold consent to settle if a claim occurs.** The captive insurance carrier provided by your employer may be making the decision whether to defend or settle your case.
3. **You may have to purchase tail coverage.** Unless your new carrier is providing prior acts coverage, you will have to purchase tail coverage. Your new employer may not cover the cost for tail coverage. Additionally, you may lose the free tail coverage that you had earned with your current carrier as well as your accrued claim-free discounts.
4. **You may lose access to a physician-focused defense.** For instance, if you are insured by a hospital's captive insurer, its attorneys will have expertise in defending hospitals, but may not have expertise in defending physicians. TMLT claim staff and defense attorneys specialize in defending physicians in lawsuits. Does the hospital's insurance company have a claims philosophy that focuses on individual physicians' risk exposures independent of the hospital's organizational interests? Who will be protecting your career in the event of a claim or lawsuit?

IN ADDITION:

5. **What if there are conflicts of interest in a lawsuit?** The potential for conflict exists in certain cases when you share a defense with your employer's appointed counsel (i.e., a joint defense). Can you be certain such conflicts will be resolved in your interest rather than that of the employer who may retain certain control over the insurance carrier? This could even lead to settlement of a defensible case.
6. **What if there are disciplinary proceedings?** Will the policy reimburse you for expenses to defend a Texas Medical Board investigation or peer review complaint? What if the hospital or employer has initiated the disciplinary proceeding against you? Who will represent you?
7. **Will you have enough coverage?** Is the aggregate limit on the employer's policy a group aggregate? If there are several significant claims filed during the policy year, will the available limits be sufficient for your claim? What happens if they are not?
8. **What about "moonlighting" coverage?** If you perform activities outside of your employment, do you have to purchase coverage for these activities at your own expense? Will you be assuming the liability of your employer under a hold-harmless and indemnification clause for these outside activities?
9. **What happens if there is a voluntary or involuntary termination?** If the contract contains a non-compete covenant, you may have to leave the area and practice elsewhere. Or, you may have to exercise the buy-out option (which could be a year's salary) in order to practice in the same area. Will tail coverage or prior acts be available and affordable at the time of separation? Will you be able to obtain a copy of your individual loss history for the period of your employment?
10. **Beware of any promises not made in writing.** The employer can change the employment contract when due for renewal. What they may offer now or agree to accommodate today could be taken away tomorrow — and if you don't like the changes or you have decided you no longer wish to be under an employment agreement, you may find it difficult to exit and still be able to practice medicine in your desired location.

[Read more](#)



Contact John Southrey, Business Development Coordinator
john-southrey@tmlt.org • 800-580-8658 x5976 • www.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, Senior Vice President, Claim Operations
 Don Chow, Senior Vice President, Marketing
 Dana Leidig, Vice President, Communications & Advertising
 Sue Mills, Vice President, Claim Operations

Associate Editor

Louise Walling

Staff

Michele Luckie

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. Available at <http://www.modernmedicine.com/modernmedicine/Modern+Medicine+Now/What-the-HITECH-Act-means-for-you/ArticleStandard/Article/detail/662044>. Accessed July 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