

## Failure to diagnose and treat hypertension

by Michele Luckie, Senior Risk Management Specialist

*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

In February 2003, a 9-year-old girl became a new patient of the practice where her parent was employed. Her previous medical records showed a well-documented history of recurrent allergies, sinusitis, upper respiratory infections, and various childhood ailments. In addition, the patient had a longstanding complaint of migraine headaches without any noted work up from her previous physician.

### Physician action

In February 2003, Pediatrician A treated the patient for allergic rhinitis and conjunctivitis. Pediatrician A prescribed cetirizine and dexamethasone eye drops. There was no record of the patient's blood pressure for this visit. The patient's parent was instructed to bring her back to the clinic in 10 days; however, there was no indication that a follow-up visit occurred. In June 2003, Pediatrician A treated the child for ear pain, fever, and vomiting. Her temperature was 99.8 degrees, but the patient's blood pressure was not measured at this visit. The results of the rapid strep test were negative, and the patient was given an antibiotic and eardrops. Pediatrician A instructed the patient's parent to bring her back in three days; there was no documentation that a follow-up visit occurred.

In December 2003, Pediatrician B treated the child for sinus congestion, headache, cough, and right ear pain. A temperature of 97.6 was recorded, but no blood pressure reading was documented. Pediatrician B prescribed amoxicillin clavulanate for sinusitis and upper respiratory infection. The patient's parent was told to return to the office as needed.

Approximately two weeks later, Pediatrician A treated the patient for cough, congestion, sore throat, fever, sores around her mouth, and lethargy for the past two weeks. Recorded vital signs included a temperature of 98.7 degrees and a pulse of 72. There was no blood pressure reading. Pediatrician A's assessment was upper respiratory infection, ulcerative stomatitis, and pharyngitis. The patient was given an antibiotic, cough medicine, and an oral paste for the sores around her mouth. The parent did not bring the child in for a re-check.

In January 2004, the child returned to the clinic with complaints of a sudden onset of bilateral hip and interior thigh pain. The parent reported that the pain was so severe that the patient could barely walk. Documented vital signs were: temperature of 99.9 degrees; pulse of 88; and respirations of 18. There

*continued on page 2*

*continued from page 1*

was no recorded blood pressure measurement at this visit. Pediatrician C saw the child and noted a benign funduscopic examination of the eyes, the presence of all peripheral pulses with normal amplitude, and a notation that no bruits were heard. There was no bruit heard over the abdominal aorta. Lab work was ordered and a prednisone dose pack was prescribed. The lab results were unremarkable with the exception of an 8.1 aldolase with the upper limit of normal being 8.0.

The first week in February, Pediatrician A saw the patient for complaints of frequent migraines. Pediatrician A noted that the patient had been complaining of a headache for 4-6 weeks with nasal symptoms and a sore throat. His assessment was sinusitis, headache, and stress. He did not order imaging of the sinuses. Pediatrician A prescribed amoxicillin clavulanate and cetirizine with instructions to follow up in two days.

The child returned five days later and was seen by Pediatrician A. The patient reported nausea and severe headaches for the past two days. Her temperature was 95.8 degrees and her pulse was 102. The patient's blood pressure was not recorded, and she was noted to be in mild distress. She was given a dose of promethazine for nausea. Pediatrician A ordered a CT scan of the head and sinuses. The patient was told to return the next day for the results.

The following day, Pediatrician A spoke with the radiologist who told him the patient was being transferred to the hospital. The CT scan showed an abnormality within the right interior pons, measuring 1.7cm x 0.7 cm. The appearance was non-specific, but the differential could include a tumor or vascular malformation.

According to the medical records, the child experienced a seizure upon completion of the CT scan. She was admitted to the hospital with chronic headaches and seizure. The patient had severe hypertension with systolic blood pressure readings in the range of 230-260 mm/Hg, which resulted in bilateral pontine hemorrhage. Physicians intubated the patient and performed an ultrasound. The ultrasound revealed a hypoplastic left kidney and bilateral renal artery stenosis. These findings were identified as the source of hypertension. Based on the echocardiogram, the physicians diagnosed chronic hypertrophy and hypertension.

Once the patient was stabilized, physicians performed a left nephrectomy and right renal artery bypass. The pontine hemorrhage around the brainstem caused quadriplegia and coma. The patient showed signs of locked-in syndrome with some recognition.

The patient remained in the ICU for more than a month until she was transferred to a specialty hospital. Upon transfer, physicians made the principle diagnosis of stroke secondary to hypertension and bilateral renal artery stenosis, brain stem hemorrhage, Rancho Stage II Coma (generalized response to stimulation and total assistance), and quadriplegia. The following family history was taken: maternal great-aunt and maternal grandmother suffered from stroke, and maternal grandfather suffered from hypertension and diabetes.

The patient remained at the specialty hospital for three months before being discharged to skilled nursing home health care. She is unable to walk or talk. Other than eye movement, she is unable to communicate.

### Allegations

A lawsuit was filed against Pediatricians A, B, and C, and the entity that employed them. The plaintiffs alleged the physicians failed to timely diagnose and treat hypertension.

### Legal implications

The plaintiff's experts claimed the pediatricians' treatment fell below the standard of care. It was argued that a thorough medical or family history was never taken and the patient's blood pressure was never recorded. Additionally, the plaintiffs' experts were critical of the pediatricians for failing to refer the patient to a specialist. They alleged the pediatrician handled each encounter independently without consideration to previous complaints or treatments.

Defense consultants were less critical of the pediatricians' actions, indicating that hypertension and renal stenosis are exceedingly uncommon in young children. However they agreed the physicians' failure to record the patient's blood pressure was a weakness, as blood pressure measurement should be part of a well-child exam.

### Risk management considerations

Taking a baseline blood pressure measurement would have alerted the physicians to the severity of the patient's condition. Vital signs are an essential part of the physical exam. While it may not be standard practice to take blood pressure at all pediatric office visits, blood pressure should be recorded at annual visits so physicians can assess any variances.

The lack of a thorough, documented medical history in the medical record affected the defense of this case. Documentation and review of a complete medical history is necessary to build a strong foundation for a patient's care. This information should be obtained during the initial visit, and include family and social history. It should be periodically updated during subsequent visits.

Finally, there was an issue of patient noncompliance in this case. While patients share the responsibility of caring for themselves, physicians should clearly communicate when patients need to follow up. Support staff should review the no-show list to determine the patient's condition and whether a follow-up phone call or letter is necessary. Documentation of follow-ups should be kept in the patient's medical record. A follow-up process shows the physician is conscientious and thorough, and it can be helpful in defending a malpractice claim.

### Disposition

This case was settled on behalf of Pediatricians A, B, and C.

*Michele Luckie can be reached at [michele-luckie@tmlt.org](mailto:michele-luckie@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.)<sup>1</sup>

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.<sup>1</sup>

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."<sup>2</sup>

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.<sup>3</sup>

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.<sup>4</sup>

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.<sup>5</sup>

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](mailto:laura-brockway@tmlt.org)  
[www.tmlt.org](http://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."<sup>6</sup>

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.<sup>5</sup>

**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](http://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.