

# the REPORTER

NEUROLOGY 2011

## Failure to restart anticoagulants

by Cathy Bryant, 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 66-year-old man came to an internal medicine physician with a complaint of shuffling gait. He had a complex medical history, including a history of stroke. The internal medicine physician referred the patient to a neurologist. Before the patient's scheduled appointment with the neurologist, the patient was admitted to the hospital with increasing weakness of the lower extremities. A cardiac work-up was completed and cardiac insufficiency was diagnosed.

### Physician action

Two weeks after the initial referral, the neurologist saw the patient. A neurologic examination was documented as hyperreflexia of the lower extremities (later this was reported to be a transcription error and should have read hyporeflexia). Also noted on the exam was decreased sensation in both feet. Differential diagnosis at this time included chronic polyneuropathy with a suspicion for chronic inflammatory demyelinating polyneuropathy and normal pressure hydrocephalus (NPH).

The neurologist ordered lab work, nerve conduction studies, and a lumbar puncture. The neurologist noted that he would call the patient's cardiologist to discuss stopping the patient's warfarin before the lumbar puncture. There is no documentation of a phone call between the neurologist and the cardiologist. Before the lumbar puncture could be done, the patient developed a viral illness and was admitted to the hospital under the care of a hospitalist.

Following this hospital stay, the patient returned to the neurologist. The neurologist dictated a letter to the patient's

internal medicine physician and the patient's cardiologist that nerve conduction studies showed decreased reflexes and that a lumbar puncture had been scheduled.

During his deposition, the neurologist stated that he instructed the patient and family to stop the warfarin; however, these instructions were not documented in the medical record.

The lumbar puncture under fluoroscopy was completed as an outpatient procedure at a local hospital. The patient did not report any problems to the neurologist during a post-procedure phone call. There was no mention in the medical record about the patient's warfarin. The hospital records did not include any discharge instructions given by the neurologist or the hospital staff.

Seven days after the lumbar puncture, the patient returned to the neurologist. Analysis of the spinal fluid revealed protein 40mg/dL; WBC 18 (100% lymphocytes); and glucose 51mg/dL. The neurologist confirmed the diagnosis of Guillain-Barre Syndrome with cervical canal stenosis. The neurologist recommended treatment with IVIG. There was no documented review of the patient's current medications or a documentation of a discussion about restarting the patient's warfarin.

Following this visit to the neurologist, the internal medicine physician saw the patient. Documentation from this visit did not include any discussion of the patient's medications.

Before the patient could be started on the IVIG treatment, he suffered a stroke and died.

*continued on page 2*

continued from page 1

### Allegations

Lawsuits were filed against the internal medicine physician and the neurologist. The allegations were based on the patient's discontinuation of warfarin and the failure of the physicians to address restarting the medication. The plaintiffs claimed this was the cause of the patient's CVA and death.

### Legal implications

During the investigation of this claim, there was considerable disagreement about the discontinuation of the patient's warfarin. The neurologist stated that he instructed the patient to hold the warfarin for only a few days before the lumbar puncture. The internal medicine physician, home health records, and the family all agreed that the warfarin was stopped approximately two weeks before the procedure, as instructed during the patient's first visit.

The neurologist's medical records did not make any reference to the patient's warfarin.

### Risk management considerations

Documenting the review of current medications at each office visit is good practice. This gives the physician the opportunity to identify compliance or noncompliance with medication plans. Both the neurologist and the internal medicine physician saw the patient after the procedure and had an opportunity to determine that the warfarin had not been restarted. Developing a process to document pre-procedure instructions given to patients and families is encouraged.

It is helpful to provide the patient and family with written instructions to help minimize confusion and maximize compliance with

special instructions. It is also helpful to document phone calls with the patient, the patient's family, and other practitioners. This documentation provides valuable information to subsequent treaters and may play an important role in the defense of the case, if litigation occurs.

Good communication between caregivers is a valuable tool for the management of patients on anticoagulants. When multiple physicians are involved in the care of a patient, it is helpful to determine and document who will be responsible for the management of the anticoagulation therapy. With outpatient procedures, it is important to communicate post-procedure instructions to be included in the patient's discharge instructions.

Complex medical problems, multiple medications, and a complement of medical specialists may result in confusion for patients and their families. This can lead to noncompliance with the medical management plan. In this closed claim, the discontinuation of warfarin to facilitate a lumbar puncture may have contributed to the patient's subsequent CVA. Communication between providers and patients is essential to ensure compliance. Documentation in the medical record of special instructions and patient/family understanding of them is important in the defense of insured physicians.

### Disposition

This case was settled on behalf of the neurologist. The case against the family physician was dismissed.

*Cathy Bryant can be reached at [cathy-bryant@tmlt.org](mailto:cathy-bryant@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.)<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/coveredentities/hitechact.pdf>. Accessed July 20, 2010.