

## Failure to diagnose surgical complications

by Louise Walling, 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 woman was referred to Surgeon A due to repeated episodes of bright red blood in her stools. She reported no pain with the bleeding, but had some abdominal pain periodically. The patient's medical history included fatigue, epilepsy, arthritis/joint pain, reflex sympathetic dystrophy (RSD) in the upper extremities, anemia, blood in stools, and change in bowel habits. Her family history included that her father had died of cancer and her brother suffered from polyps and diverticular disease.

### Physician action

Nearly a month later, Surgeon A performed a colonoscopy on the patient at a local hospital. Prior to the procedure, the risks, benefits and complications were explained and the patient's consent was obtained. The dictated procedure report described the passage of the scope as "somewhat difficult." Two sessile polyps were removed. The patient's recovery was uneventful and she was discharged from the hospital. She was given discharge instructions to contact the surgeon with any complaints of severe abdominal pain, nausea, vomiting, rectal bleeding, or fever.

Progress notes from Surgeon A's office reflect that the patient called that evening complaining of cramping abdominal pains. Surgeon A thought the problem was probably related to colon insufflation during the procedure. Instructions on conservative measures were given.

Nearly 24 hours later, the patient called the office complaining of persistent spasms. Surgeon A requested that she come to the office for an examination and for abdominal films. He ordered a KUB. He reviewed the films with the radiologist, and concluded that they were essentially normal. Documentation from this visit shows that the patient was afebrile, complaining of diffuse abdominal pain with muscle spasms, which were aggravated by body motion, primarily when moving from standing to a sitting position. Guarding was present with the muscle spasms without rebounding. She had no abdominal distention and bowel sounds were present.

*continued on page 2*

*continued from page 1*

Surgeon A noted that the patient's abdominal spasms were possibly related to her RSD. He prescribed an injection of meperidine and promethazine for relief of her symptoms. She was asked to notify him with any persistent problems. Additionally, he referred her to her regular physician for further evaluation for possible complications of her RSD.

Two days later, the patient was admitted to another hospital by her primary care physician. Here she was diagnosed with an acute surgical abdomen as indicated by a low WBC count with a left shift and CT scan results indicating a perforation of the proximal ascending colon with marked contamination of the peritoneal cavity. Surgeon B performed a resection of the distal ileum and proximal colon with anastomosis. Post-operatively the patient developed sepsis and infection. Within a few days the patient was taken back to the OR for re-exploration. Several pelvic and subhepatic abscesses were found and drained. Surgeon B also found that the previous anastomosis was disrupted. A second resection of the distal portion of the ileum and proximal colon and re-anastomosis of the two was performed.

Several months later, the patient's post-operative course was complicated by an incisional hernia, which Surgeon B repaired. The patient also claimed that her pre-existing RDS was aggravated. Surgeon B followed this patient for nearly eight months.

### Allegations

A lawsuit was filed against Surgeon A, claiming that his actions were negligent and grossly negligent as follows:

- causing a bowel perforation and/or similar and/or related injuries to plaintiff during the course of surgery;
- failing to exercise reasonable care to avoid such injuries;
- failing to timely, adequately and/or properly treat the plaintiff;
- undertaking to provide medical care and treatment without sufficient qualification;
- failing to consult with and/or refer plaintiff to other more qualified physicians in a timely and appropriate fashion; and
- failing to act as an ordinarily prudent physician would have acted under the same or similar circumstances.

### Legal implications

The plaintiff's expert was critical of Surgeon A for referring the patient back to her primary care physician. At a minimum, he felt that there should have been communication from Surgeon A that included an ongoing evaluation. He was critical of the order of a KUB rather than a CT, and for giving the patient narcotic pain medication. He argued that had Surgeon A kept the patient in the hospital for observation and kept her NPO, an earlier diagnosis may have led to a less complicated recovery.

Three defense experts, two of whom were not supportive, reviewed this case. Each noted that perforation of the colon during a colonoscopy is a known complication as outlined in the informed consent. To Surgeon A's credit, he saw the patient soon after she began voicing complaints. However, Surgeon A failed to recognize that the patient's discomfort was unusual. One of the defense experts had concerns that Surgeon A did not order a CBC or admit the patient for observation. Also, the medical records did not provide adequate evidence that the patient was properly followed after her post-operative complaints.

### Risk management considerations

During deposition, Surgeon B stated that he understood why Surgeon A had missed the patient's complaint of abdominal cramping as a sign of a bowel perforation. Her medical history included chronic pain, and he believed the patient reacted to pain in a way that most people would not. Perhaps this created risk for Surgeon A. Viewing the patient's post-colonoscopy complaint within the context of her medical history and in relation to the procedure may have provided the right answers. A documented phone call from Surgeon A to the primary care physician when he referred the patient for complications of her RSD may have been helpful as well.

### Disposition

The case was settled on behalf of Surgeon A.

*Louise Walling can be reached at [louise-walling@tmlt.org](mailto:louise-walling@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>**

# 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**

Bob Fields, President and CEO  
 Jill McLain, Executive Vice President, Claim Operations & Risk Management  
 Don Chow, Senior Vice President, Marketing  
 Dana Leidig, Vice President, Communications & Advertising  
 Sue Mills, Vice President, Claim Operations

**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. 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](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.