Failure to communicate risks of medication

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 24-year-old woman came to her family physician reporting symptoms of depression, hypersomnia, crying spells, fatigue, and loss of appetite. She informed her physician that her grandparents had recently died. The patient denied having suicidal thoughts, and the physician prescribed bupropion 150 mg daily for 14 days. The patient was also given the name of a psychiatrist and several psychologists so she could seek counseling.

According to medical records, this patient initially came to the practice four years earlier requesting a prescription for oral contraceptives. The physician continued to see her for well-woman exams, oral contraceptives, and occasional flare ups of acne and psoriasis.

Physician action

Two weeks passed, and the patient came for a follow-up visit. She was diagnosed with resolving depression. Her current dose of bupropion 150 mg daily was continued and she was given a 30-day prescription.

The patient returned a month later. She reported improvement overall and relief of depressive symptoms. Her prescription of bupropion 150 mg daily was refilled for three weeks. Thereafter, she was to increase the dose to 300 mg daily and return for a re-check in five days.

Over the next several weeks, the patient continued her follow-up visits for depression. During one of these visits, she disclosed that she had been smoking marijuana and drinking alcohol. The family physician strongly encouraged her to discontinue use of illicit drugs and alcohol. He refilled her prescription for bupropion 300 mg.

At the next visit — nearly six weeks later — the patient reported that the medication was no longer helping. The physician strongly encouraged her to see another physician, preferably a psychiatrist. He provided her with two referral names. There was no medication prescription documented at this visit.

After seeing a psychiatrist, the patient returned to the defendant physician for a follow-up visit. She reported that she had seen a psychiatrist, and that he discontinued bupropion and placed her on

continued on page 2
buspirone. At this visit, she was diagnosed with social anxiety disorder and prescribed paroxetine 12.5 mg, 1 to 2 tablets daily.

Three weeks passed and the patient called the office requesting samples of paroxetine, indicating that she was out of medication. She was told that they did not have any samples. The patient was given an appointment the next day; she did not show for this appointment.

Nearly two weeks later, the patient’s mother came to the office requesting a prescription for paroxetine for her daughter. She reported that the medication was working well. Samples were not available, so the physician wrote a 30-day prescription.

Over the next 18 months, the patient was seen at the clinic for a well-woman exam and oral contraceptives. Her mental health status was not documented at these visits, nor were prescriptions given for antidepressants.

Nearly four years after her initial complaints of depression, the patient returned to the family physician. Her chief complaints were severe menstrual cramps, anxiety, and nervousness, which she stated she had been experiencing for five years. The physician provided the patient with a 3-week supply of escitalopram 10 mg.

Six weeks later, the patient’s mother called the practice and spoke with the physician’s nurse. She reported that the patient had committed suicide two days earlier.

Allegations
The patient’s parents filed a lawsuit against the family physician. They alleged that the actions of the defendant were negligent and proximately caused the patient’s death. The allegations included:

- prescribing escitalopram to someone in the patient’s condition;
- failure to communicate the increased risk of suicidal behavior associated with patients in this age range who take this medication;
- failure to follow up with the patient; and
- failure to refer the patient to a specialist.

Legal implications
Defense experts who reviewed this case could not support the defendant’s care. Their comments were focused particularly on the sparse documentation and illegibility of his entries, primarily on the last visit. Elements missing from the documentation of this visit were a physical exam, psychiatric exam, an assessment of suicidal thoughts or plans, a discussion of antidepressant medication risks and benefits, a referral for further counseling or psychiatric treatment, and when the patient was to return for follow-up care to assess her progress with the new medication.

Risk management considerations
Primary care physicians are frequently the first health care professionals to hear patients’ complaints of depressive symptoms and requests for help. Because primary care physicians treat patients over many years, they become familiar with patients’ families, times of stress, crisis, and loss. During these times, the demands for a physician’s care may be increased. It is wise to remember that although years of medical history and treatment create a familiarity that may not be documented, there are critical, objective elements of record keeping that should not be compromised. It is recommended that physicians document the patient’s report of symptoms of depression, anxiety, and assess whether the patient has suicidal thoughts or plans. This helps establish the reason for the diagnosis, and helps explain the choice of medication. It is also good risk management practice to document referral sources for counseling or psychiatric treatment for patients with a history of mental health issues.

A verbal informed consent discussion about the benefits of the medication, side effects, and the risks associated with taking the medication — which should also be documented — can assist in helping patients understand what to expect. This also demonstrates the physician’s efforts to educate and treat patients.

As a way to document that the patient was told to return, indicate the need for a follow-up visit in the treatment plan. Another suggestion is to ask the patient to schedule the follow-up visit when the patient checks out. Not all patients will schedule their next appointment at this time, but this can assist the majority of patients in complying with follow-up care.

Disposition
The claim against the family physician was dropped. The statute of limitations expired and a lawsuit was not filed.

Louise Walling can be reached at louise-walling@tmlt.org.

---

*continued from page 1*

---

**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.)

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 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.

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.”

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.

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.

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.

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,
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 unsecured 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


