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 the physicians led to allegations of professional liability, and how risk management techniques may have either prevented the outcome or increased the physician’s defensibility. This study has been modified to protect the privacy of the physicians and the patient.

PRESENTATION
In March 2010, a 60-year-old man came to a pain management physician for treatment of chronic neck and back pain, spastic gait, and spasticity in his upper extremities. He had a complex medical history of fibromyalgia, lupus, irritable bowel syndrome, migraines, asthma, arthritis, deep vein thrombosis, restless leg syndrome, and obesity. He was on multiple medications, including cyclobenzaprine for pain and muscle spasms.

PHYSICIAN ACTION
The pain management physician prescribed tramadol for pain and baclofen for muscle spasms. Over the next two months, the physician also performed injections of pain medication into the patient’s hip, back, and neck with minimal relief.

In April 2010, the patient consulted with his neurologist who recommended discontinuing the cyclobenzaprine in favor of the new baclofen prescription. The same month, the patient returned to the pain management clinic and was seen by the physician assistant (PA). The PA felt that the patient was benefiting from the two muscle relaxers and continued treatment with cyclobenzaprine and baclofen. At this time, the patient complained of daytime sleepiness and the PA began treatment with armodafinil.

In July 2010, due to ongoing daytime sleepiness and inability to sleep, the patient saw a sleep medicine specialist. Sleep studies indicated complex sleep apnea. Bilevel positive airway pressure (BPAP) was prescribed.

On August 27, 2012, the sleep medicine specialist started the patient on 4-hydroxybutanoic acid. Recognizing the need for caution due to the patient’s current medication regimen, the sleep medicine specialist advised the patient to take other depressant medications earlier in the evening before taking the 4-hydroxybutanoic acid at 11 pm. The patient took the 4-hydroxybutanoic acid at 11 pm and then a second dose at 3 am. When the patient began the 4-hydroxybutanoic acid prescription, he was also taking tramadol, cyclobenzaprine,
The scope of practice by altering the physician prescribed regimen. Additionally, the experts felt that the PA exceeded to the substantial change to the patient's narcotic treatment much input was provided by the pain management physician. All of the experts agreed that it was difficult to establish how morphine therapy with 4-hydroxybutanoic acid.

medicine specialist about possible interactions of fentanyl or to gradually increase the dosage of morphine. They also felt it would have been prudent for the PA given the complexity of this case, there were mixed opinions among experts who reviewed the case for TMLT.

On January 15, 2015, the patient returned to the pain management clinic and reported that the fentanyl patches did not control the pain. The PA discontinued the fentanyl patches and prescribed 20mg of morphine every 12 hours for seven days. The patient was advised to increase the morphine after seven days to 40mg every 12 hours if pain was not well controlled. The PA also prescribed acetaminophen and hydrocodone, up to two per day, as needed for breakthrough pain. The pain management physician signed the prescriptions.

On January 25, 2015, the patient increased the dose of morphine. At 3 am, the following morning, the patient’s wife noticed the patient was not breathing. EMS was called, but the patient could not be revived. He was pronounced dead.

ALLEGATIONS
A lawsuit was filed against the pain management physician, the PA, and the pain management clinic. The suit alleged:

- negligence by the PA for changing the prescription regimen without consultation with the pain management physician and without documenting medical reasoning for the change;
- negligence by the pain management physician for signing off on the prescription change without a patient evaluation; and
- failure of the pain management physician and the pain management clinic to properly supervise the PA.

LEGAL IMPLICATIONS
Given the complexity of this case, there were mixed opinions among experts who reviewed the case for TMLT.

The experts believed it would have been prudent for the PA to gradually increase the dosage of morphine. They also felt it may have been beneficial for the PA to consult with the sleep medicine specialist about possible interactions of fentanyl or morphine therapy with 4-hydroxybutanoic acid.

All of the experts agreed that it was difficult to establish how much input was provided by the pain management physician to the substantial change to the patient’s narcotic treatment regimen. Additionally, the experts felt that the PA exceeded the scope of practice by altering the physician prescribed regime without consulting the pain management physician or documenting the medical decision making for the change.

The experts were also critical of the pain management physician for signing prescriptions without evaluating the patient or reviewing the patient's chart. Furthermore, the experts were concerned the pain management physician had not seen the patient for at least two years and that the PA was managing a complex narcotic medication regimen without proper physician involvement.

Additionally, the pain management clinic was criticized for not having policies and procedures for the management of narcotic medication regimens with physician oversight.

DISPOSITION
This case was settled on behalf of the pain management physician, the PA, and the pain management clinic.

RISK MANAGEMENT CONSIDERATIONS
The patient in this case had numerous chronic conditions and a complex medication regimen, which highlighted the lack of involvement and treatment of the pain management physician. The lack of consultation by the PA with the pain management physician also created concerns with this case. The pain management clinic could have benefited from policies and procedures that included:

- Scope of practice and delegated prescriptive authority for physician assistants.
- Protocols for physician assistants to consult supervising physicians and document medical decision-making when narcotic medication regimes are significantly changed.
- Protocols for review of charts by supervising physicians.
- Guidelines for consulting with other treating providers/physicians on patients with complex medical histories and narcotic medication regimens.
- Review of Texas Medical Board rules regarding the supervision of mid-level practitioners (both physician’s assistants and advanced practice nurses), found in chapters 185 and 193.6 of the Texas Administrative Code, and Section 157 of the Occupations Code. (Sources below.)

SOURCES

Kassie Toerner can be reached at kassie-toerner@tmlt.org.
Cyber security issues continue to be a major burden for physicians and health care facilities. Data breach incidents, including patient identity theft, are on the rise and can be devastating.

Below is a case study based on alleged violations of HIPAA privacy rules. This study describes how actions by physicians or their employees led to the allegations, and how risk management techniques may have prevented the violations. The ultimate goal in publishing this study is to help physicians comply with privacy and security standards.

**PATIENTS IDENTIFIED ON SURGEON’S WEBSITE**

A plastic surgeon’s website featured “before and after” photos of patients. The patients’ names were not used and the photos were posted in a way that preserved patient anonymity.

However, unknown to the plastic surgeon and his staff, the patients’ names had not been properly removed from the meta tags associated with the photos. Meta tags are content descriptors that describe web page content to search engines. Meta tags do not appear on the page, but are found in the HTML code for the page.

The issue was discovered when a patient performed a Google search on herself and her images from the plastic surgeon’s site appeared in the search results. Although he was told about the meta tag issue, the plastic surgeon did not immediately remove the photos. Fifteen patients filed lawsuits against the plastic surgeon. The Office of Civil Rights also investigated the plastic surgeon for possible HIPAA violations.

**RISK MANAGEMENT CONSIDERATIONS**

When patient photographs are completely de-identified, HIPAA requirements are satisfied. If patient photos are not de-identified, written authorization from the patient is required to post or share the photos.

To de-identify a photo based on the HIPAA Safe Harbor de-identification standard, the following identifiers of the individual or of relatives, employers, or household members of the individual, must be removed:

1. “Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
   a. The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
   b. The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
3. All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Vehicle identifiers and serial numbers, including license plate numbers
6. Fax numbers
7. Device identifiers and serial numbers
8. Email addresses
9. Web universal resource locators (URLs)
10. Social security numbers
11. Internet protocol (IP) addresses
12. Medical record numbers
13. Biometric identifiers, including finger and voice prints
14. Health plan beneficiary numbers
15. Full-face photographs and any comparable images
16. Account numbers
17. Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and
18. Certificate/license numbers."

OTHER RISK MANAGEMENT TIPS
• Obtain patient consent to take photographs. Specify how you plan to use the photos (i.e. medical records only, marketing, website, journal article) on the consent form.
• Do not name or save photo files with any of the above identifiable information in any publicly accessible area. (Clearly, if you are just adding photos to medical records, they can contain identification.)
• Audit photos that have been added to your website. Check the site page for tags, meta tags, keywords, or anything that could be used to identify patients.
• Do not store photos of patients in an unencrypted device, such as a camera, cell phone, tablet, or personal laptop.

TMLT COVERAGE
For incidents alleging violations of HIPAA, TMLT policyholders are protected under Medefense and cyber liability coverage, both offered with every TMLT policy.

Medefense reimburses or directly pays the legal expenses incurred by a physician from a disciplinary proceeding, including violations of HIPAA. Fines and penalties arising out of such disciplinary proceedings are also covered on a reimbursement basis only.

Cyber liability coverage protects against claims arising from the theft, loss, or unauthorized access of both electronic and physical health information. The coverage also includes payment of regulatory fines and penalties and covers the cost of data recovery and patient notification.

TMLT also offers fee-based services to help minimize cyber threats, including violations of medical privacy and security laws. Our cyber risk management services include HIPAA risk assessments; IT services; policy and procedure reviews; publications; and customized training.

For more information, please visit the TMLT cyber consulting services website at www.tmlt.org/mlt/products-services/cyber-consulting-services.html.

To report a claim under Medefense or cyber liability coverage, please contact the TMLT claim department at 800-580-8658.

"(c) Implementation specifications: re-identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

(1) Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and
(2) Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification."

SOURCE

Laura Brockway can be reached at laura-brockway@tmlt.org.

Robin Desrocher can be reached at robin-desrocher@tmlt.org.