FAILURE TO DIAGNOSE AND TREAT ACUTE CORONARY SYNDROME

PRESENTATION
At approximately 9:30 am, a 43-year-old man came to the emergency department (ED) of a metropolitan hospital. He had complaints of chest pain, dizziness, diaphoresis, shortness of breath, and pain going down his arms. The pain had been intermittent for the last three days, and had increased in intensity over the last few hours.

PHYSICIAN ACTION
An emergency medicine physician examined the patient and documented that he stated his pain was exacerbated by movement and relieved by rest. The patient further stated that he had been “lifting at work all day.” The patient was pain free when he came to the ED.

The patient had a history of hypertension and occasional cigar smoking. He had no family history of cardiac disease. Upon exam, his blood pressure was 148/100 mm Hg; his pulse rate was 67 bpm; and he had a normal respiratory rate of 18.

Chest x-ray and EKG results were normal. The CBC was normal with mild hemoconcentration of hemoglobin 18.8 g/dl and hematocrit of 54%. With the exception of an elevated AST level of 51, the results of the complete metabolic panel were normal. Cardiac enzymes were also reported as normal. The emergency medicine physician concluded that the patient had chest wall and neuropathic pain.

The patient was discharged at 12:45 p.m. with instructions to take a daily aspirin and follow up with his primary care physician in one to two days for a stress test. The patient was to return to the ED if his condition worsened. At the time of discharge, the patient reported no pain and his vital signs were satisfactory.

Early the next morning, the patient’s wife found him pulseless and apneic in his car. EMS was called and, upon their arrival at the scene, the patient was in full arrest. Down time before the arrival of EMS was estimated to be 10 to 15 minutes. Despite resuscitation efforts, the patient remained asystolic until his arrival at the hospital. The same emergency physician treated the patient. Chest compressions and Advanced Cardiovascular Life Support (ACLS) methods were continued without success. The patient died.

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.
An autopsy revealed cardiomegaly, left ventricular hypertrophy, and 100% stenosis in the left anterior descending coronary artery.

ALLEGATIONS
The patient’s family filed a lawsuit against the emergency medicine physician. The suit alleged that the patient was misdiagnosed with chest wall and neuropathic pain, and then inappropriately discharged.

Serial EKGs, cardiac enzymes, and a cardiac stress test or coronary angiography could have assisted the physician to timely diagnose and treat the patient. The patient was discharged after one EKG and two sets of cardiac enzymes less than two hours apart.

Plaintiffs alleged that the standard of care was breached when: a.) the physician failed to admit the patient to an inpatient monitored unit; b.) a full dose of aspirin was not given to the patient while still in the ED; and c.) a cardiology consult was not obtained prior to discharge.

LEGAL IMPLICATIONS
Physicians who reviewed this case for the defense were mixed in their opinions. The majority stated that, given the patient’s initial complaints, he required admission to the hospital for a cardiac workup; serial EKGs should have been performed; and an adult dose of aspirin should have been administered.

DISPOSITION
The case was settled on behalf of the emergency medicine physician.

RISK MANAGEMENT CONSIDERATIONS
The patient’s chest pain included an atypical feature — sharp pain that became worse with movement. But it was also accompanied with typical signs of cardiac chest pain, namely, chest pain radiating to the arms, diaphoresis, shortness of breath, hypertension, and obesity.

The patient’s combination of symptoms, a normal EKG, and normal cardiac enzymes should have prompted further action on the part of the emergency medicine physician. The need for serial enzymes, serial EKGs, a cardiology consult, and further cardiac testing and monitoring would have required the patient to be admitted to a monitored bed for 24 hours.

Emergency departments assist physicians by implementing detailed, time-sensitive chest pain protocols. While a missed diagnosis of acute coronary ischemia is a common allegation against emergency medicine physicians, protocols have their limits and do not address every possible patient scenario.

Physicians are encouraged to look at the larger perspective and include the patient’s medical history and all reported symptoms. Consider the worst possible outcome in a patient reporting chest pain. In this case, the emergency physician may have been prompted to administer aspirin, order serial EKGs and cardiac enzymes, a cardiology consult, and admit the patient to a monitored unit.

Louise Walling can be reached at louise-walling@tmlt.org.
CASE CLOSED: HIPAA AND PATIENT PRIVACY

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.