CARDIOLOGY

2017

the REPORTER

TMLT
Texas Medical Liability Trust

By Sara Bergmanson, Digital and Social Media Specialist, and Louise Walling, Senior Risk Management Representative

FAILURE TO PROPERLY SUPERVISE AND TREAT CONSERVATIVELY

PRESENTATION

A 74-year-old woman visited Cardiologist A with symptoms of congestive heart failure. She had a history of dilated cardiomyopathy, mitral valve regurgitation, and significant pulmonary hypertension. An electrocardiogram (EKG) revealed significant left ventricular dysfunction with moderate mitral valve regurgitation, and an apical thrombus in the left ventricle.

PHYSICIAN ACTION

After his evaluation, Cardiologist A recommended right and left heart revascularization with possible defibrillator placement, and warfarin therapy. Two days later, the patient was taken to surgery.

While performing the surgery, Cardiologist A was assisted by Cardiologist B who was part of a university fellowship program. Cardiologist A's staff privileges included training and supervising Cardiologist B.

Upon performing the left heart catheterization, Cardiologist A found that the left internal mammary artery and left anterior descending artery were unobstructed. He proceeded with a percutaneous transluminal coronary angioplasty. These actions were not noted in the operative report or medical record.

Cardiologist A placed the stent in the first diagonal artery. While preparing the stent for the main artery, Cardiologist A noticed a slight spasm. He instructed Cardiologist B to give nitroglycerin to relax the heart muscles. Cardiologist B administered the nitroglycerin through a catheter with a saline flush. Seconds later, Cardiologist A noticed the QRS complex of the EKG began to widen and the patient went into ventricular fibrillation and then cardiac arrest. The catheter was pulled, and Cardiologist A noticed the saline flush coming out of it. He realized that Cardiologist B had not closed the saline flush valve after giving the nitroglycerin.

CPR was administered for approximately 30 minutes. Once the patient stabilized, Cardiologist A checked the diagonal artery for patency and found no evidence of stent thrombosis. He spoke with the family about continuing the procedure, although they deny the discussion took place.

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.

He then proceeded with a left main stent followed by intra-aortic balloon pump. The patient's hemodynamic condition improved and a temporary pacemaker was placed.

The patient was transferred to the Critical Care Unit, but became unresponsive once she arrived. She was placed on mechanical ventilation and was hypoxic for approximately 30 minutes with saturations of 88% down to 84%. There was no gag reflex and she was not considered a candidate for hypothermic protocol secondary to prolonged hypoxemia.

The patient never regained consciousness nor had any improvement in neurological function. She remained in a vegetative state and died less than a year later.

ALLEGATIONS

The family filed a lawsuit against Cardiologist A alleging:

- failure to treat the patient conservatively before attempting a high risk, invasive procedure;
- failure to supervise Cardiologist B;
- failure to disclose Cardiologist B's actions to them; and
- failure to properly document his actions in the medical record.

LEGAL IMPLICATIONS

Consultants for the plaintiff did not agree with Cardiologist A's decision to proceed with an invasive procedure that was not medically necessary. Defense consultants expressed similar concerns. Cardiologist A's lack of documentation in the medical chart also affected his credibility. In addition, the family testified they were not informed of Cardiologist B's involvement until after they filed suit.

Cardiologist A admitted in deposition that he had control over all of Cardiologist B's actions due to his responsibilities in supervising and training cardiac fellows in the university fellowship program. This included telling the cardiac fellow to shut the valve after administering the nitroglycerin during the catheterization procedure.

DISPOSITION

Given the multiple defense challenges, this case was settled on behalf of Cardiologist A.

RISK MANAGEMENT CONSIDERATIONS

When Cardiologist A accepted the responsibility of supervising and training cardiologists in the fellowship program, he assumed vicarious liability for these cardiologists. Vicarious liability extends liability beyond the original defendant to a person or entity responsible for the defendant's actions. In this case, Cardiologist A was vicariously liable for the actions of Cardiologist B.

Procedure notes should accurately reflect the details of the procedure, including any complications. Effort should be made to avoid a documentation approach that, apart from the date, makes each procedure read the same. Templates can be used; however, prepopulating the script can make the notes appear as if the physician was hurried and did not take time to accurately document what happened during a procedure. A thoroughly documented procedure note provides a good reference should the physician need to recall details of his course of actions and may also be valuable to subsequent treating physicians.

Fully documenting discussions with patients and family members is also important in the event of a bad outcome. In the record, include who was present, what matters were discussed, decisions made, and outstanding matters, along with the date, location, and time. Guidance on how to best document patient and family discussions and decisions in the patient's records may be attained from a qualified attorney. Hospitals and other large providers usually employ legal counsel to provide such guidance.

Sara Bergmanson can be reached at sara-bergmanson@tmlt.org

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

By Laura Hale Brockway, ELS, Assistant Vice President, Marketing, and Robin Desrocher, BSN, RN, CPHRM, Manager, Risk Management

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."[1]

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/tmlt/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.[1]"

SOURCE

1. U.S. Department of Health and Human Services. Guidance regarding methods for de-identification of protected health information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Available at http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/#standard. Accessed September 1, 2016.

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

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

TMLT
Texas Medical Liability Trust