FAILURE TO REPORT MISPLACED CENTRAL LINE

PRESENTATION
On July 22, a 64-year-old woman came to the emergency department (ED) of a local hospital. The patient had undergone back surgery five days earlier, and she came to the ED for a possible accidental overdose of pain medication. She exhibited signs of altered mental status, acting differently, and trouble concentrating.

The patient’s history included COPD, hypertension, congestive heart failure, obstructive sleep apnea, and chronic lower back pain. Her vital signs were blood pressure 70/40 mm Hg; pulse 90; respirations 20; and temperature of 99.5 degrees.

Shortly after arriving in the ED, she vomited a large amount of black coffee emesis. Emergency Physician A intubated the patient and inserted a central line in the right subclavian vein. Hospitalist A admitted the patient to the ICU.

PHYSICIAN ACTION
Hospitalist A requested a pulmonary consult, and Pulmonologist A saw the patient on July 23. Pulmonologist A reviewed a chest x-ray taken of the patient the day before. He confirmed that the patient had pneumonia. Pulmonologist A’s differential diagnosis was acute respiratory failure, aspiration pneumonia, sepsis related to aspiration, and COPD.

Pulmonologist A ordered to continue IV fluids and maintain the patient’s central venous pressure (CVP) at 6- to 8- cm of water. At 10 a.m., a nurse contacted Pulmonologist A and told him the patient’s CVP was in the 70s. Pulmonologist A assumed the central line was kinked and could still be used to deliver medication to the patient. Pulmonologist A left the hospital the evening of July 23 and did not return until July 28.

Chest x-rays were taken every day from July 22 to July 28. Radiologist A read the chest films taken on July 22, 27, and 28. He did not mention the central line on July 22, but on the 27 and 28 reports he stated it was uncertain whether the line was in an artery or vein. Radiologist B read the chest film on July 23 and reported that the catheter tip appeared to be in the right innominate vein. Radiologist C read the chest films from July 24-28. On each of her reports, she recommended the subclavian line be repositioned as the tip of the catheter crossed the midline.

When Pulmonologist A returned on July 28, he reviewed the chest films and thought the tip of the central line was coming out. He ordered a peripherally inserted central catheter...
(PICC) line. Arterial blood gas measurements confirmed the central line was in the artery, not the subclavian vein as documented.

When the patient's sedation was lightened in anticipation of a possible extubation, she was found to have weakness and decreased mobility on her left side. The misplaced subclavian line was removed.

The patient was transferred to a regional hospital, where she was found to have an embolic acute infarct predominantly in the right middle cerebral artery territory, secondary to a misplaced line.

Upon discharge, the patient had left-sided weakness, no use of her left arm, a left foot drop, and cognitive deficits. She received physical and occupational therapy at a skilled nursing facility. The patient now has left arm hemiparesis, but is reported to be doing well.

**ALLEGATIONS**

Lawsuits were filed against Pulmonologist A, Hospitalist A, and Radiologists A, B, and C. The allegations against the radiologists involved failure to diagnose that the central line was in the artery and not a vein, and failure to report their findings to the referring physicians.

**LEGAL IMPLICATIONS**

Three defense consultants reviewed the care given by the treating radiologists. All of the consultants stated that it was not possible to tell if a catheter is in an arterial or venous system based only on a chest x-ray. Therefore, their interpretations of the x-rays were accurate and met the standard of care.

The consultants were critical of Emergency Physician A, who placed the line. They indicated that it is fairly easy to determine if the line is in the arterial or venous system at the time of placement. Further, it would have been the attending physician's responsibility to follow up on placement, not a radiologist's.

The main criticism against the radiologists involved their failure to call the treating physicians and emphasize the need to re-check the line placement. However, the treating physicians testified that they were aware of the radiologist reports indicating that the line was not in a good position, but took no action to re-position the line.

**DISPOSITION**

Though experts testified that the radiologists met the standard of care, there was concern about the potential for an adverse jury verdict. Therefore, this case was settled on behalf of the three radiologists, Pulmonologist A, and Hospitalist A.

**RISK MANAGEMENT CONSIDERATIONS**

In non-routine clinical situations, the radiologist should expedite delivery of report findings and communicate directly with the ordering physician. Also, the American College of Radiology's *Guidelines for Communication of Diagnostic Imaging Findings* offers instructions for creating a complete diagnostic imaging report. Two guidelines apply in this case:

- Clinical issues: the report should address or answer any specific clinical questions. Factors that prevent answering the clinical questions should be clearly stated.
- Impression (conclusion or diagnosis): follow-up or additional diagnostic studies to clarify or confirm the impression should be suggested when appropriate.

Situations that may warrant non-routine communication include cases that occur in critical care units that involve the findings of a significantly misplaced line or tube. Findings that may affect patient care if not treated in a timely fashion, and are unexpected by the ordering physician, would also fall into this category.

It is a best practice for interpreting physicians to document all non-routine communications in the radiology report with the date, time, method of communication, and name of the person receiving the report.¹

Unfortunately, when a case involves several physicians, poor communication can be an issue. There are several ways to communicate in today's electronic age, but having a conversation with the patient's health care provider and following up by documenting the conversation may provide the radiologist with context for future studies.

**SOURCE**


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

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.