Good Medicine Deserves to Be Defended

By John T. Ryman, JD

“Do a good turn daily.” – BSA Scout slogan

The sky was filled with twinkling blue-white stars promising a fair day ahead when Dr. Able [1] climbed into his car to head for the hospital. A 70’s classics station played unnoticed in the background as Dr. Able mentally reviewed his schedule of neurosurgical cases for the day. Always meticulous, he was already preparing to do his best.

Later that morning, Dr. Able was wrapping up a scheduled surgical case when he was asked by a nurse from Dr. Baker’s OR if he could help Dr. Baker. Dr. Able told the nurse he would be glad to help and would come to Dr. Baker’s OR as soon as he finished his case.

Dr. Able arrived at Dr. Baker’s OR to find that he had the patient in the prone position and had started thoracic spine surgery. Dr. Baker is an orthopedic surgeon. Dr. Able reviewed

the MRI which showed a very large, herniated disc. Dr. Baker was having trouble removing the disc. Dr. Baker did not have a preoperative CT scan, which Dr. Able would have routinely obtained. Dr. Able scrubbed in. He quickly realized the surgery would be difficult, but he thought it could be safely completed. Dr. Baker assisted as Dr. Able worked on removing the disc. Near the end of the case, while removing bone fragments, the neuro monitoring tech noted that they had lost signal to the legs. He was using SSEP spinal cord neurologic monitoring. It was thought this change might be anesthesia-related. Dr. Able finished his part, turned the case back over to Dr. Baker to close, and moved to his next case. After finishing his next case, Dr. Able consulted with Dr. Baker about the patient. The news was not good. The patient could not move her legs. An MRI was ordered STAT which showed remaining disc material and significant stenosis. Doctors Able and Baker decided to promptly return the patient to surgery after getting consent from the patient's spouse. During the second surgery they attempted to further decompress the area. Following this second surgery, an MRI showed continued narrowing and compression. Both doctors thought they had decompressed as much as safely possible, and further surgery would be unreasonably risky for the patient. The patient remained paralyzed in her legs.

"No good deed goes unpunished." – Oscar Wilde

The patient filed suit against both Dr. Able and Dr. Baker. She alleged that Dr. Baker deviated from the standard of care by attempting to perform surgery from a posterior approach and that Dr. Able deviated from the standard of care by continuing with the approach and failing to open a sufficiently wide exposure. She alleged that Dr. Able should have ended the surgery and referred the patient to another surgeon or returned the patient to surgery later with a different approach. These alleged failures by Dr. Baker and Dr. Able caused the injury to her spinal cord and resulting paraplegia. In short, the plaintiff alleged that the approach selected by Dr. Baker was a deviation from the standard of care, continuation of the surgery was a deviation by Dr. Able, and these deviations caused the patient to be permanently paralyzed.

The case proceeded through the typical lengthy discovery process. The plaintiff produced a neurosurgery expert who criticized Dr. Baker for attempting to perform surgery on the patient from a posterior approach. The expert was critical of Dr. Able for continuing the surgery and failing to extend the exposure. According to this expert the deviation from the standard of care caused the injury to the plaintiff's spinal cord and resulting paraplegia.

The plaintiff alleged multi-million-dollar damages and made a settlement demand commensurate with the claimed damages. The settlement demand was considered but declined by both doctors.

The healthcare provider defendant is almost always the most important witness in any case. Dr. Able was a very good witness who had the ability to effectively educate the jury. The consulting medical experts are also very important. Both doctors had qualified experts to explain to the jury that the care was appropriate and within the standard of care. The expert for Dr. Able was one of the top neurosurgeons in the nation and had worked with

Dr. Able in the past. He proved to be a very convincing expert.

Both defendants were represented by experienced defense counsel, who had taken many cases to trial. These attorneys were among the best of the best.

This case went to trial about four years after the surgery, and both Dr. Able and Dr. Baker were defendants at trial. It was undisputed that the paraplegia was permanent and occurred during the surgery. The plaintiff's experts had significantly different opinions about key issues in the case, including timing of the injury and the specific approach that should have been used. These discrepancies may have made the plaintiff's experts seem less credible. In contrast, the defense experts were more consistent. They were also more experienced in the type of surgery done on this patient. Consequently, when communicating with the jury, they seemed more confident about the surgery and their opinions.

The trial lasted eight days. After all evidence had been presented, the jury found that there was no negligence by either Dr. Able or Dr. Baker. Based on the jury findings, the Court dismissed the plaintiff's case against Dr. Able and Dr. Baker with prejudice.

Even with the best of intentions and medical care, sometimes bad things happen. It does not necessarily mean that there was any negligence by the practitioner. SVMIC brings the resources and commitment to tell your story of competence and caring. In this case, that carried the day.

[1] Names have been changed.

Cybersecurity Resources to Protect Your Practice

By Loretta Verbeck, MS, FACMPE, CHC

It is difficult to make it through an entire week without a new cyberattack making the news. The FBI reported in their 2020 Internet Crime Report 791,790 complaints regarding cybercrime last year, representing an increase of more than 300,000 over 2019. The reported losses from these crimes exceeded $4.1 billion. By some estimates, only 15% of cybercrimes are reported, meaning the actual number of victims may be 1.5 to 2.5 million. Phishing scams, ransomware, and server attacks continue to impact individuals and businesses, with the business of medicine maintaining a high spot on the list.

Healthcare organizations must be diligent in their efforts to protect the systems that contain protected health information (PHI) and other sensitive information, such as employee personally identifiable information (PII), from cybercrime attacks. However, understanding the necessary steps and implementing the appropriate safeguards to

manage cybersecurity can be overwhelming for many practices.

To assist policyholders with the daunting task of cybersecurity, SVMIC is committed to providing members with resources, including a series of articles that will guide policyholders through the steps necessary to develop an effective cybersecurity program. Topics will include:

- Security Risk Analysis
- The Importance of Proper System Backups
- Understanding Cyber Liability Coverage
- Ransomware
- Using Technology to Secure Systems
- Responding to Security Incidents

SVMIC has partnered with Tokio Marine HCC to provide all policyholders with cyber liability coverage and cybersecurity resources through CyberNET. To access these resources, visit this link which will require you to log in to your Vantage® account. Here you will find sample security policies, resources for responding to security incidents, cybersecurity training videos, and more.

Because ransomware and email fraud are two of the most common cyberattacks, CyberNET provides critical information on both topics.

Top 8 Ways to Beat Ransomware is an eight-step checklist including:

1. Training videos for employees
2. Detailed information to assist with remote desktop protocol (RDP) and access control
3. Instructions for installing software patches
4. Information on creating effective backups
5. Implementing two-factor authentication
6. Installing and updating anti-virus programs
7. Instructions for email security settings
8. Installing an endpoint security program

Top 5 Ways to Protect Against Business Email Compromise (BEC) is a five-step checklist including:

1. Implementing two-factor authentication
2. Detailed information to prevent fraudulent wire transfers
3. Training videos for employees
4. Configuring email systems to filter out phishing emails automatically
5. Installing an endpoint security program

The Department of Health and Human Services, Office for Civil Rights (OCR), is responsible for enforcing HIPAA Security Rule violations, which are frequently associated

with cybersecurity incidents. As a part of Security Rule compliance, all workforce members must receive ongoing security awareness training. By utilizing these resources, you can train your workforce, protect your organization from a cybersecurity incident, **and** meet existing Security Rule requirements.

Even with these resources, it can be a challenge to implement safeguards if you are not a technology expert. The good news that by utilizing the CyberNET resources, you have access to pre-paid cybersecurity experts who can provide guidance. Should you need more advice than your policy covers, the cybersecurity expert can refer you to other sources of information or consultants who can work with you on your cybersecurity program.

These resources are provided as a value-added benefit by SVMIC as a part of your cyber liability policy, and policyholders are strongly encouraged to take advantage of them. Doing so can help reduce the risk of a cyberattack and the financial and reputational damage that typically follows a successful attack.

Our mission at SVMIC is to protect, support, and advocate for physicians and other healthcare providers. Providing members with these and other resources to address cybersecurity is one way we accomplish this mission.

If you have questions about cybersecurity or access to these resources, call 800-342-2239 or email contactsvmic@svmic.com.

If you experience a cybersecurity incident, contact the SVMIC Claims Department as soon as possible by calling 800-342-2239.

Other individuals in your organization may benefit from these articles and resources, such as your administrator, privacy or security officer, or information technology professional. They can sign up for a Vantage account here.

Risk Matters: Unsolicited Test Reports

By Jeffrey A. Woods, JD

When an unsolicited test result is received regarding an established patient of the practice, it should be handled the same way as one that was personally ordered. Contact the patient, notify the ordering physician, and, if appropriate, arrange for needed follow-up care. Do not automatically assume normal results do not require action, as occasionally results within normal range of the laboratory may not be the expected result for the patient. Additionally, notify the testing facility that the provider is not the ordering physician, and that the result should be delivered to the physician who ordered the test.

If the patient is *not known* to the provider, there is still a limited duty of care owed to the patient. Much of this obligation would be minimized by confirming with the ordering physician (if possible) that he or she received and addressed the test result. In any event, notify the testing facility that the provider is in receipt of the report in error, and that it should be delivered to the ordering physician. If the report indicates a panic value or grave condition and the provider is not able to confirm the ordering physician is in receipt of the report, an attempt to contact the patient would be appropriate for patient safety

considerations. In both cases, it is important to document all steps taken to correct the error.

Sequestration Holiday Extended

By Elizabeth Woodcock, MBA, FACMPE, CPC

The Centers for Medicare & Medicaid Services (CMS) put a temporary hold on Medicare claims in March. The pause in processing resulted from pending legislation to extend the removal of the 2% sequestration cut to Medicare reimbursement. On April 13, Congress voted to continue the sequestration relief through the end of the year. Signed into law the next day, the move by the federal government was welcomed by physicians across the nation. No delay in payment processing is expected as a result of the temporary hold.
