Closed Claim Review: Good Things Come for Those Who Persevere

By William "Mike" J. Johnson, JD

The rural surgeon took the patient to surgery around midnight. Her condition was miserable: relentless nausea, vomiting, and dry retching. The hour may have been late, but the patient was prepped and had been NPO after a previously done scope. The surgeon had placed the patient on several antiemetics, and he wanted to give those time to work, but the patient changed her mind and asked him to operate. She was tired of dry retching.

Approximately four years earlier, the patient had undergone an elective laparoscopic Roux-en-Y gastric bypass by a different surgeon. She was in her forties, morbidly obese, smoked two packs of cigarettes per day, and suffered from hypertension and chronic bronchitis. Her post-operative course after the gastric bypass surgery was uneventful. Prior to the gastric bypass, she was hospitalized for paresthesia of her right arm and leg. Approximately three years after her gastric bypass, the patient began a repetitive course of hospitalizations for nausea and vomiting.

During one of the hospitalizations, the surgeon in this case performed an EGD which showed gastric anastomotic ulcers at the site of the prior gastric bypass and the formation of a blind pouch at the site of the jejunum and the stomach pouch. An incisional hernia was also discovered. Several days later the surgeon performed a laparotomy in which he excised the blind pouch, explored the anastomosis, repaired the incisional hernia, and lysed adhesions. Her immediate postoperative course was uneventful; however, about two weeks later she was hospitalized for severe nausea and vomiting. The patient underwent numerous workups and tests. The anastomosis was narrowing; ulcers appeared to be the culprit. Thus, the surgeon cut the vagus nerves to the stomach to keep the ulcers from coming back, removed the old anastomosis, and created a new anastomosis so that food could pass through. Nonetheless, the patient's persistent nausea and vomiting continued.

During the surgery that is the focus of this suit, the surgeon considered that the patient could have an efferent blind loop of the residual stomach. A CT scan showed the residual nonfunctional stomach to be dilated and distended. A significant portion of the patient's stomach was disconnected from the gastric pouch. The residual nonfunctional stomach was created in the original gastric bypass surgery by stapling across the stomach and connecting the residual upper part of the stomach to the bowel thus creating the gastric pouch; it currently served no purpose. An informed consent was obtained, and the surgeon removed the stomach remnant –the gastric pouch the bariatric surgeon previously created was not removed. An examination of the stomach remnant by the surgeon did not reveal any obvious problems: no issues with the mucosa, no tumors, and the pyloris was grossly unremarkable. Pathology indicated active gastritis with reactive epithelial changes. The nausea and vomiting completely stopped for eight days.

However, eight days later the patient returned to the hospital with nausea and vomiting. During this encounter, the patient was observed by a nurse putting her finger down her throat to make herself vomit. The patient said this helped relieve pressure on her stomach. The patient continued to be hospitalized for nausea and vomiting. An allergy to Lortab was considered, and the surgeon noted that while the patient complained of persistent nausea, he never saw her vomit in his presence.

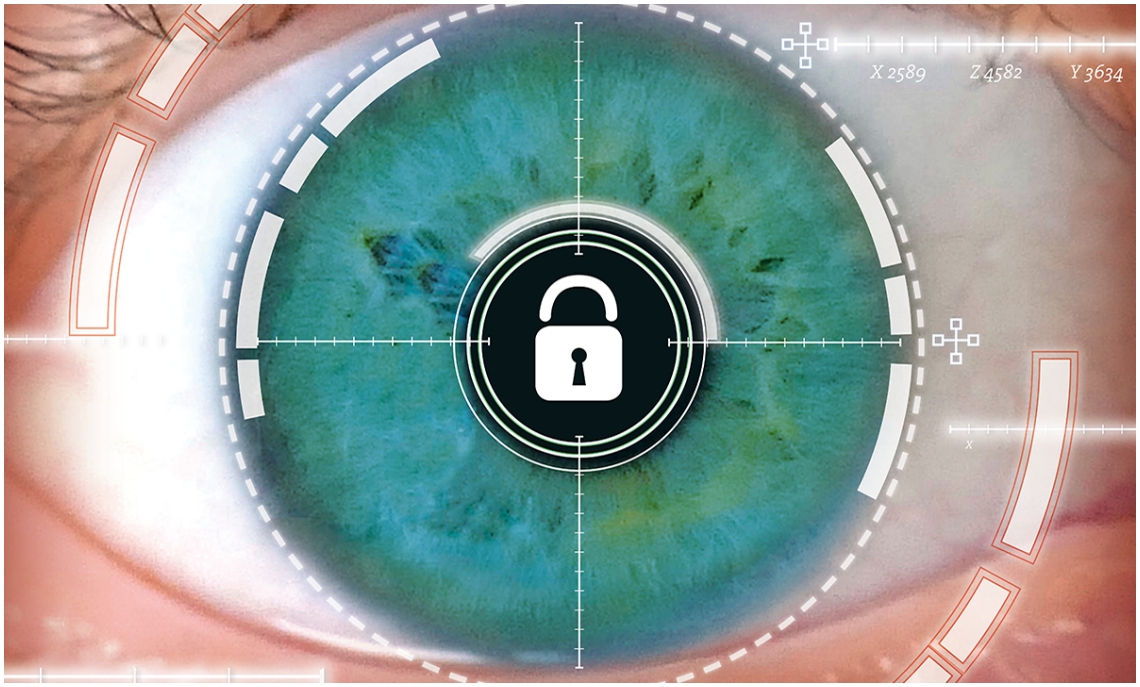
In the lawsuit the patient alleged that the surgeon failed to consider alternative surgical treatments that were less drastic than removing the stomach, failed to obtain informed consent before completely removing her stomach, and removed her stomach based on an erroneous assumption that she was suffering from an efferent blind loop of the residual

stomach.

Defending this case presented several challenges. The surgeon had treated the patient during several hospitalizations without success which could subject him to criticism for not referring her back to the bariatric surgeon. The surgery to remove the stomach remnant was only two weeks after the surgeon performed the reconstruction of the anastomosis. For this he could be criticized as being too aggressive, not allowing time for further evaluation and conservative treatments before performing another major surgery. Another potential criticism was whether surgery to remove the remnant was justified. Some words the surgeon used in his charting were problematic. In particular, in his records he stated that he performed a total gastrectomy or removal of the stomach when in fact he only removed the remnant portion—not the portion fashioned by the bariatric surgeon. The fact the surgery began so late in the evening seemed unorthodox for nonemergent surgery, and while the surgeon contended that he obtained informed consent, the patient had been on morphine and other drugs which could undermine the validity of the consent. The plaintiffs had expert witnesses to support their criticisms of the care.

Despite the challenges, there were strong points. Foremost, the surgeon was absolutely steadfast in his desire to go to trial. Two very good experts supported the surgeon on the standard of care and causation aspects of the case. They were very effective witnesses at trial as was the defendant surgeon. The surgeon is a long-term member of the community, is well-liked, and has earned a reputation for credibility. A defense verdict was returned after two hours of deliberation. Some comments after the trial included that the surgeon is considered to be an excellent physician, and a potential juror commented that this surgeon had prayed with him before he underwent surgery. Although the patient's treatment course had been long and complicated and certain aspects of the care were criticized, the jury believed that the surgeon had the patient's best interests at heart and used his skill and expertise to try to improve her condition. With the defense verdict, they confirmed the surgeon's belief that he had met the standard of care in his treatment of the patient. Defending the case took a great deal of time, effort, and an emotional toll on the surgeon, but it was worth it in the end when the jury confirmed that he had made the right decisions in treating the plaintiff and in defending his care through trial.

Ransomware 2.0 - The New Generation of Ransomware



By Rana McSpadden, FACMPE

On May 7, 2021, the U.S. felt firsthand the consequences of a ransomware attack when the Colonial Pipeline Company was hacked by the criminal cybergroup DarkSide. This hack disrupted a major infrastructure system and caused panic for many Americans. Even though Colonial Pipeline paid the $4.4 million ransom, the pipeline remained offline for several days as IT experts worked to clean and restore the network.

Prior to the Colonial Pipeline hack, third-party service provider MedNetwoRX (which services Aprima's electronic medical records system) reported a ransomware attack on April 22, 2021[i] that affected some clients for more than two weeks. These clients scrambled to implement emergency procedures so they could continue serving their patients. As a result of the attack, patient records and schedules were rendered inaccessible. Affected practices did not know who would be coming in that day and could not schedule new patients nor could they access patient contact information to reschedule non-emergency visits for a later date. Without access to records, patient care was put at

risk since providers could not access histories, allergy lists, or medication lists. The attack, likewise, disrupted cash flow as affected practices were unable to submit claims. To these practices, this attack was just as devastating as the Colonial Pipeline attack.

According to a recent report from Check Point, there has been a 57%[ii] increase in ransomware attacks since the beginning of 2021, with healthcare being the number one affected industry. On average, healthcare organizations see 109 attempted attacks each week. Of course, large corporations are not the only groups at risk for ransomware attacks. An estimated 43%[iii] of all cyberattacks target small businesses. This is generally because small businesses lack the funding for strong internal cybersecurity programs staffed with full-time cybersecurity professionals and layers of the latest security technology. However, the relatively smaller cybersecurity budget of private medical practices does not mean that smaller practices necessarily have to be at greater risk. The first step to a good cybersecurity program is to know your risks and educate staff. In Justin Joy's June 2020 article, he outlined how practices should leverage the HIPAA Security Rule to help defend against these threats.

Emerging Ransomware Trends

Original ransomware tactics were to deposit malicious software into systems, either through phishing email scams that infect files or by downloaded software which would encrypt (lock up) the victims' systems. Then attackers would demand payment to unlock the system. For many victims, it was easier to pay the ransom than try to restore their system, particularly if they did not have adequate backups in place. As groups began instituting better system backups from which they could restore their systems, this original tactic began losing effectiveness. To combat this, hackers began using double extortion tactics. They began exfiltrating data from their victims' computers prior to encrypting the systems. Demand notices began informing victims to either pay the ransom or their data would be released to the dark web. They would send the victims proof of the data they stole. As a result of this new tactic, hackers saw a 171%[iv] increase in ransom payments. To increase their profits even further, towards the end of 2020 and into 2021, hackers began implementing triple extortion tactics. With this, not only does the initial victim receive a demand for payment, but their patients and customers whose data was involved in the theft also receive demand emails. Finally, in recent months, if ransomware victims fail to pay the ransom, some hackers have started deploying Distributed Denial of Service (DDoS) attacks, as well as making threatening phone calls to victims to encourage payment. A DDoS attack is where hackers flood a victim's network with malicious traffic that keeps the victim's system from communicating or working as it should. It is unknown how widespread these emerging trends are, but it is always necessary to remain vigilant.

Responding to Ransomware

Prevention is always the best policy, but what if you are the victim of a ransomware attack? What should you do? **Do not pay the ransom**. Contact SVMIC so that we can activate your cyberliability policy and put you in touch with Tokio Marine (our third-party cyberliability insurer) to speak with their legal experts. Each attack is unique, and the

response will vary based on the situation. Once Tokio Marine is involved, they will walk you through next steps which may include reaching out to IT professionals to get you up and running while still preserving evidence. Of course, paying the ransom may be a last resort but should **ONLY** be done under the direction of the experts at Tokio Marine.

Finally, the determination of whether a HIPAA breach has occurred because of the ransomware attack requires a legal analysis, often made based on findings from a digital forensic investigation and other information specific to the incident. If the determination is made that a breach has occurred, assistance will also be provided with the breach notification process, including notification to various federal and state government bodies (if applicable).

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

If you experience a cybersecurity incident, contact SVMIC as soon as possible by calling 800-342-2239 and ask to speak to the Claims department.

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.

[i] https://www.healthcareitnews.com/news/reported-ransomware-attack-leads-weeks-aprima-ehr-outages

[ii] https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/

[iii] https://purplesec.us/resources/cyber-security-statistics/ransomware/#:~:text=The%20Growing%20Threat%20Of%20Ransomware&text=Ransomware%20has

[iv] https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/

Hold Harmless: MIPS Cost Category

By Elizabeth Woodcock, MBA, FACMPE, CPC

On May 20, 2021, the Centers for Medicare & Medicaid Services announced that the hotly debated cost category will be reweighted to 0% for 2020, effectively eliminating it from scoring as part of the Merit-based Incentive Payment System (MIPS). Advocates for physicians – including the American Medical Association – had advocated for the reweighting based on the impact of the COVID-19 pandemic. This announcement only applies to those physicians who participated in the program. Many physicians did not report to the program in 2020, which will not impose the expected penalties in 2022 for non-participation based on the pandemic.

The 2021 exception applications are now open, should you wish to take steps to eliminate your participation (and any penalty) this year. Because the pandemic is considered an "extreme and uncontrollable circumstance," any physician can apply for the exception. Should you change your mind, the program will set aside the exception application, so it makes for a great back-up plan. The penalty is a substantial 9% (applied to all Medicare payments) for non-participants in perpetuity, so it should be on your calendar to participate each year – or submit that application.

Risk Matters: Wrong-Site, Wrong-Procedure, and Wrong-Patient Surgery

By Jeffrey A. Woods, JD

Few medical errors are as indefensible as those involving patients who have undergone surgery on the wrong body part, undergone the incorrect procedure, or had a procedure performed that was intended for another patient. These “wrong-site, wrong-procedure, wrong-patient errors” (WSPEs) are termed “never events” by the National Quality Forum and “sentinel events” by the Joint Commission– errors that should never occur and indicate serious underlying safety problems. In addition, the Centers for Medicare and Medicaid Services (CMS) will not reimburse hospitals for any costs associated with WSPEs. Yet, these “never events” continue to occur.

The official website of the Department of Health & Human Services, in an article updated September 2019, noted that although one seminal study indicated that such errors occur in approximately 1 of 112,000 surgical procedures, that estimate only included procedures performed in the operating room; if procedures performed in other settings (ambulatory surgery centers and interventional radiology suites, for example) are included, the rate would be significantly higher. A study conducted using Veteran Affairs data found that fully

half of the WSPEs occurred during procedures outside the operating room.

Root cause analyses of WSPEs consistently reveal communication issues as a prominent underlying factor. The Joint Commission's Universal Protocol attempts to address these communication issues through redundant mechanisms for verification of the correct site, procedure, and patient as well as site marking, checklists, and "timeouts." However, even when Universal Protocols are implemented, errors can still happen well before the patient reaches the operating room, a timeout is rushed, or production pressures contribute to errors during the procedure itself. As the above-cited article points out, ultimately, preventing WSPEs depends on a combination of system solutions, strong teamwork, a safety culture, and individual vigilance.

SpeakUP™

The Universal Protocol

for Preventing Wrong Site, Wrong Procedure, and Wrong Person Surgery™

Guidance for health care professionals

Conduct a pre-procedure verification process

Address missing information or discrepancies before starting the procedure.

- Verify the correct procedure, for the correct patient, at the correct site.
- When possible, involve the patient in the verification process.
- Identify the items that must be available for the procedure.
- Use a standardized list to verify the availability of items for the procedure. (It is not necessary to document that the list was used for each patient.) At a minimum, these items include:
  - ❑ relevant documentation
    Examples: history and physical, signed consent form, preanesthesia assessment
  - ❑ labeled diagnostic and radiology test results that are properly displayed
    Examples: radiology images and scans, pathology reports, biopsy reports
  - ❑ any required blood products, implants, devices, special equipment
- Match the items that are to be available in the procedure area to the patient.

Mark the procedure site

At a minimum, mark the site when there is more than one possible location for the procedure and when performing the procedure in a different location could harm the patient.

- For spinal procedures: Mark the general spinal region on the skin. Special intraoperative imaging techniques may be used to locate and mark the exact vertebral level.
- Mark the site before the procedure is performed.
- If possible, involve the patient in the site marking process.
- The site is marked by a licensed independent practitioner who is ultimately accountable for the procedure and will be present when the procedure is performed.
- In limited circumstances, site marking may be delegated to some medical residents, physician assistants (P.A.), or advanced practice registered nurses (A.P.R.N.).
- Ultimately, the licensed independent practitioner is accountable for the procedure – even when delegating site marking.
- The mark is unambiguous and is used consistently throughout the organization.
- The mark is made at or near the procedure site.
- The mark is sufficiently permanent to be visible after skin preparation and draping.
- Adhesive markers are not the sole means of marking the site.
- For patients who refuse site marking or when it is technically or anatomically impossible or impractical to mark the site (see examples below): Use your organization's written, alternative process to ensure that the correct site is operated on. Examples of situations that involve alternative processes:
  - ❑ mucosal surfaces or perineum
  - ❑ minimal access procedures treating a lateralized internal organ, whether percutaneous or through a natural orifice
  - ❑ teeth
  - ❑ premature infants, for whom the mark may cause a permanent tattoo

Perform a time-out

The procedure is not started until all questions or concerns are resolved.

- Conduct a time-out immediately before starting the invasive procedure or making the incision.
- A designated member of the team starts the time-out.
- The time-out is standardized.
- The time-out involves the immediate members of the procedure team: the individual performing the procedure, anesthesia providers, circulating nurse, operating room technician, and other active participants who will be participating in the procedure from the beginning.
- All relevant members of the procedure team actively communicate during the time-out.
- During the time-out, the team members agree, at a minimum, on the following:
  - ❑ correct patient identity
  - ❑ correct site
  - ❑ procedure to be done
- When the same patient has two or more procedures: If the person performing the procedure changes, another time-out needs to be performed before starting each procedure.
- Document the completion of the time-out. The organization determines the amount and type of documentation.

This document has been adapted from the full Universal Protocol. For specific requirements of the Universal Protocol, see The Joint Commission standards.

The contents of The Sentinel are intended for educational/informational purposes only and do not constitute legal advice. Policyholders are urged to consult with their personal attorney for legal advice, as specific legal requirements may vary from state to state and/or change over time.