Monitoring Your Revenue Cycle

By Elizabeth Woodcock, MBA, FACMPE, CPC

Ensuring the health of your revenue cycle is like self-care for your medical practice – essential to prioritize so that you can serve your community for many years to come. It's a great idea to do a full physical on your revenue cycle every three to five years, but monthly monitoring helps keep guardrails on your practice's finances. Create a template for a dashboard to maintain the pulse of your revenue cycle, and report on these key indicators:

Revenue: Ultimately, your bank account reflects the monies collected by your practice, so it's a great idea to put the revenue for the month at the top of your dashboard. Calibrate the information by dividing revenue by physician days worked or work relative value units, to make sure that your revenue is tracking with effort.

Days in receivables outstanding: If your practice has a healthy revenue cycle, your receivables management should be in good shape. To gauge success, measure your days in receivables management. Calculate this indicator by dividing your practice's average daily charge into total current receivables (net of credits). The measure, which should be 25 to 35 days (unless you have a particularly challenging payer), gives you a great lens

into the health of your revenue management.

Aged trial balance: Another excellent marker of receivables management performance is the aged trial balance, often referred to by its acronym, ATB. Typically displayed in a table format, the ATB reports the monies owed to your practice, by payer, based on 30-day time periods. If the information is too voluminous for the dashboard, consider reporting the percentage of receivables over 120 days. Compare this to the average of the previous year to ensure that it's not trending down.

First-pass clean claims rate: The addition of a revenue cycle predictor like the first-pass clean claims rate allows you to monitor your revenue cycle prospectively. Aim for a 100% pass-through rate, but recognize that insurance payers have complex, ever-changing rules that make this virtually impossible. Further, a lower-than-expected clean claims pass rate may not be undesirable. If your practice can catch problems before they pass into the payers' hands, your practice may be able to prevent denials. Consider reporting the first-pass clean claims rate, alongside the denial rate on your dashboard.

Payer mix: Unless your practice is off the (insurance) grid, and collecting directly from patients, the mixture of insurers deserves to be carefully monitored. Reimbursement from insurers represents your practice's revenue potential. For the dashboard, it's okay to keep it at a high level. Using a pie chart, report the percent of Medicare, Medicaid, Commercial Insurers, Self-Pay, and Other. Add other categories – Workers' Compensation, for example, if they contribute a high percentage to your payer mix. The key is to monitor changes, so display the current mix adjacent to the historical one. Changes to your payer mix may be the sole reason your revenue has slipped, regardless of how effective your revenue management efforts are.

There may be other receivables management indicators that you add on your dashboard but leave room for two other elements that can add value to your monitoring efforts: (1) benchmarks for your specialty, often available from your professional society or practice management association; and (2) a qualitative narrative from your director. The addition of a subjective review of the past month offers the opportunity for management to explain the performance. The tangential benefit is that it forces directors to thoughtfully draw upon their insights – to analyze and assess concisely with intention.

The best dashboard is one that offers both a quantitative and qualitative perspective, not surprisingly given the incredible complexity of the revenue cycle.

Risk Matters: Telephone Calls

By Jeffrey A. Woods, JD

Documenting telephone encounters should be treated with the same level of importance as documenting in-person visits. Telephone conversations, particularly those that occur after-hours, are a major area of liability risk. The advice given to a patient over the telephone often becomes crucial to his or her continued care. It may also be vital in the event of a medical malpractice claim. Therefore, all telephone conversations with patients, regardless of when they are received, should be documented in the patient's medical record - both for continuity of medical care and for the defense of a potential malpractice claim. Documentation should provide a clear picture of what information was given to the patient, including follow-up instructions and information specifying when to seek emergency care. Documentation such as "spoke with patient" is not as complete as a detailed note and may hinder continuity of care and defensibility in the event of a claim.

In most cases, undocumented conversations become a "he said/she said" dispute and prolong a claim's resolution. A note recorded in the medical record on the front end can save a lot of heartache on the back end. In many cases, contemporaneous documentation of the provider's instructions would have greatly aided in the defense of a malpractice

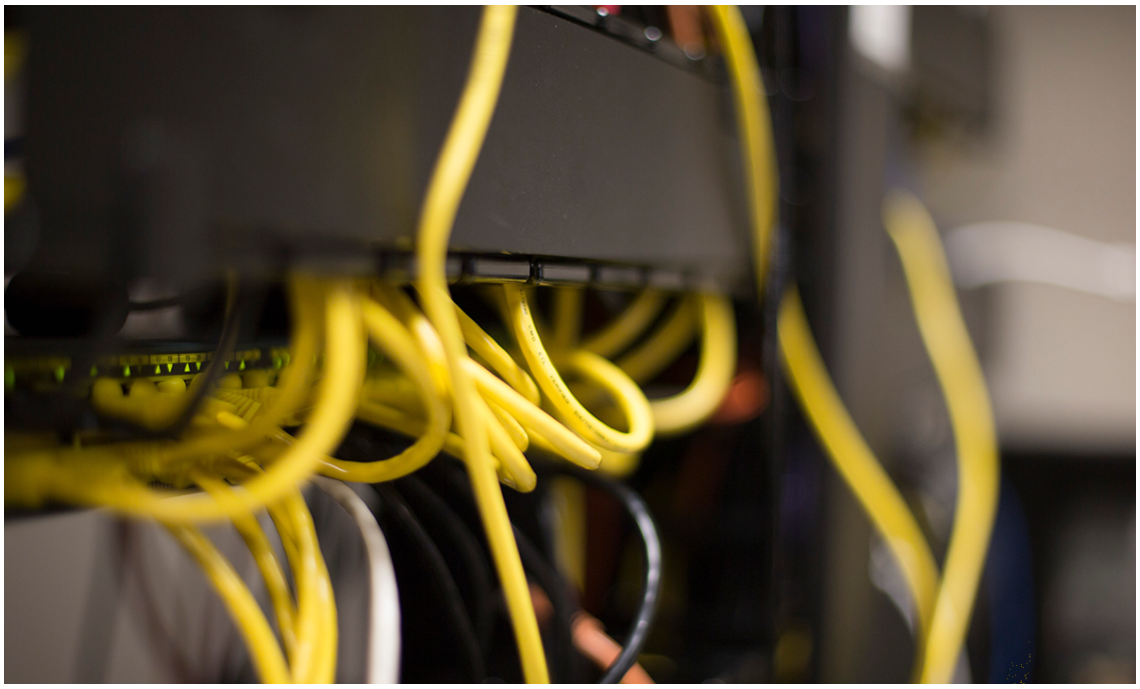
claim against the provider.

Contemporaneously documenting care is particularly crucial when documenting after-hours. Calls from a patient outside of normal office hours are often of a serious nature. Without contemporaneous documentation, the physician must rely on memory to recall the advice or recommendation given. At a minimum, the following types of phone calls need to be contemporaneously documented in the medical record:

- All phone calls in which test results are reported to patients, noting if the patient was advised to return or seek other medical attention.
- All phone calls in which the patient is advised to return or seek other medical attention, including instructions to go to the emergency department.
- All phone calls in which a patient requests medical advice or prescription refills.

To assist in the documentation of relevant phone call information, SVMIC provides phone call record forms free for members. Request them here.

Know Your Policy: Your Coverage and Responsibilities under the Cybersecurity Policy



By Sherie Edwards, J.D.

As a value-added benefit of your SVMIC professional liability policy, you and your practice are provided with $50,000 of cybersecurity coverage (with the option to purchase more coverage). This coverage, although provided by SVMIC, is written and administered by Tokio Marine Houston Casualty Company, referred to in this article as TM. As with any insurance policy, it is good to familiarize yourself with what is covered, what is excluded, and what your responsibilities are in terms of reporting an incident to be sure that you are doing all you can to maximize this benefit. This information will also be valuable in conforming your internal policies and procedures related to incident reporting to the requirements under the policy; it's better to know and be ready for an incident rather than to expend precious time scrambling to try to figure out what should be done while in the thick of a crisis.

What is Covered?

The protection provided under the Cybersecurity policy falls into two categories: First Party claim coverage and Third Party claim coverage. A First Party claim is an event that impacts your practice and/or your systems, such as a potential compromise resulting from a phishing email or ransomware attack. A Third Party claim is an event which has the potential to result in a lawsuit against your practice. An example of this would be a HIPAA breach. The nine types of coverages named in the policy are:

Coverage A: Multimedia Liability—the release or display of information on your website or in printed material for which you have sole responsibility and which results in a claim of defamation, libel, or product disparagement (list is not inclusive).

Coverage B: Security and Privacy Liability—this category includes HIPAA/HITECH breaches, data breaches that involve Personally Identifiable Information (PII), breach of government laws and regulations regarding privacy protections; a security breach that occurs due to the failure to have systems and protections in place; and unauthorized access or use of your computer systems.

Coverage C: Privacy Regulatory Defense and Penalties—covers the fines, penalties, and awards you are required to pay, by statute or regulation, that result from a security or privacy breach.

Coverage D: Privacy Breach Response Costs; Patient Notification Expenses and Patient Support; Credit Monitoring Expense—up to the limits of your coverage, pays the costs of notifying affected individuals when a privacy/security breach occurs.

Coverage E: Network Asset Protection, which includes Loss of Digital Assets and Non-Physical Business Interruption and Extra Expense—this coverage pays to restore data and computer programs to their same state and contents as they were prior to being damaged, destroyed, or stolen. This includes the time spent by your employees to recover or restore these digital assets. Non-physical business interruption includes income loss and expenses incurred while the use of your computer system is interrupted

due to a covered event (such as a phishing hack or ransomware).

Coverage F: Cyber Extortion (ransomware)—this article from our June 2021 Sentinel provides a comprehensive overview of ransomware attacks.

Coverage G: Cyber Terrorism—an act of cyber terrorism is an attack by a person or a group against computer systems, the Internet, or networks in order to cause disruption, intimidation, or otherwise cause harm. This is usually done to further a political, religious, or ideological cause. Many insurance policies, including this one, exclude damages caused by war, invasions, or insurrections; however, acts of cyber terrorism are not included in this usual exclusion.

Coverage H: PCI DSS Assessment—if you accept credit cards for payment, then you are familiar with Payment Card Industry standards, or PCI. This coverage provides protection if you are fined by a bank or credit card company in the event of a security or privacy breach that violates a PCI standard.

Coverage I: BrandGuard®—BrandGuard is the name TM gives to their coverage that protects you against decreased business income due to negative media coverage. As with all losses, there is a specific way this loss is determined, which is outlined in your Endorsement.

In some instances, the coverages listed above will extend to damages or loss caused by a third party Business Processing Outsourcing (BPO) provider or an outsourced IT service provider.

How Much Coverage Do I Receive?

The Cybersecurity policy that SVMIC provides as a benefit includes $50,000 of coverage per claim for each coverage shown above. The aggregate amount depends on the number of physicians in your group practice:

1 physician	$50,000 aggregate
2-10 physicians	$100,000 aggregate
11-20 physicians	$150,000 aggregate
21+ physicians	$250,000 aggregate

Unlike your professional liability policy, defense costs are included toward the total amount of your coverage. Also, depending on the type of coverage (D, E, F, G, and I above), claims arising from “the same, related on continuing incident(s)” will be considered as one claim. Likewise, claims made under Coverages A, B, C, and H, if considered to be

causally or logically related, will be viewed as a single claim.

What is Excluded?

Your Cybersecurity policy lists several Exclusions, and you are encouraged to read those in the Cybersecurity endorsement to your professional liability policy. A few examples of exclusions are a deliberate act or willful violation of a law; obligations under other insurance policies such as worker's compensation or any other employment matter; a liability you assume under a contract or agreement (unless you would have been liable even if a contract or agreement didn't exist); or a violation of sanctions imposed by the Federal government, including sanctions under the Office of Foreign Assets Control (OFAC).

The last exclusion mentioned above is critical as it relates to cyber extortion claims (ransomware). If a ransom payment is made to a terrorist group or another party on the OFAC sanctions list, that payment may be excluded from coverage. It may also result in criminal penalties from the Federal government. This underscores the importance of calling SVMIC to report an incident before taking **any** action on your own.

As noted earlier, this list is not all inclusive, and you should review your policy for the full list.

What are my responsibilities under the policy?

As with your professional liability policy, you have a duty to notify SVMIC of a claim or incident as soon as you are aware, whether by receiving a notice of claim from a third party or through your own discovery. The policy requires the following notices:

- For Coverages A, B, C, or H you are required to provide written notice of the claim during the policy period.
- For Coverages D, E, F, G, or I, you are required to provide written notice within 60 days of discovering (or within 60 days of when you should have reasonably discovered) a media report that is adverse, a security or privacy breach, a covered cause of loss, a cyber extortion threat, or a cyber terrorism act.

However, we strongly encourage you to contact SVMIC as soon as you know or suspect an incident has occurred, or that the potential for a claim exists. With your notice, we can place you in contact with TM who will provide the assistance (legal and technical) needed to address the issue.

It is also important to note that any payments you make or settlements you enter into before notifying SVMIC of an actual or potential incident may be excluded from coverage.

Additional Coverage

If, after reading this article you believe that $50,000 of coverage would not be adequate to protect your practice from a cybersecurity incident, please call SVMIC and ask to speak to

one of our Underwriting Specialists. They can help you obtain additional coverage.

Prevention is always the best policy

Just as the risk management education programs SVMIC provides help you decrease your professional liability risk, the cybersecurity resources you can access through Vantage® can help your practice protect itself against cybersecurity losses. These resources, offered by CyberNet and accessible via the Vantage policyholder portal, include educational materials, sample policies, information about incident response plans and business continuity plans, and news about the latest cyber threats. Just like your Cybersecurity policy, these resources are a value-added benefit of your professional liability policy with SVMIC.

If you have questions about cybersecurity or access to the resources available exclusively to SVMICmembers, call 800-342-2239 or email ContactSVMIC@svmic.com.

Individuals in your organization such as your administrator, privacy or security officer, or information technology professional may benefit from this article and the other resources available to SVMIC policyholders and staff through their Vantage account. If someone in your organization needs a Vantage account, they can sign up here.

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

Prioritize Diligent Medicine Over Events

By Jamie Wyatt, JD

Four out of five physicians say they are currently experiencing symptoms of burn out. [1] One of the biggest challenges for any working professional is finding a work-life balance. Given the current health care climate, providers are dealing with increased stressors ranging from the global pandemic, a decrease in compensation due to suspension of surgeries and elective procedures, rising costs of doing business, and loss of control over the practice of medicine due to heavy regulation. These are just some of the factors affecting overall professional contentment. The need to recharge is ever more present, but how is this accomplished while ensuring you, as a medical provider, meet your ethical obligations to refrain from abandoning your patients or a perceived abandonment outcome?

This edition of Closed Claim Review provides a good lesson on what **not** to do in handling patient calls. The patient is George Callaher[2], a 40-year-old male, who suffered with chronic back pain for years. He was referred to Dr. Strobl for consideration of a dorsal

column stimulator after he successfully completed a trial by his pain management physician. All conservative measures were taken but seemed to fail, and Mr. Callaher was deemed an appropriate candidate for the surgery. He consented to the procedure and underwent placement of a dorsal column stimulator, which was done successfully by Dr. Strobl without any complications. On the initial postoperative visit, Mr. Callaher was recovering well from the surgery. His incisions were healing well with no tenderness to palpation, no erythema, edema, open areas, nor any drainage at the incision site. It appeared his thoracic and right flank incisions were healing without issue.

Three weeks post-operatively, Mr. Callaher woke up in severe pain and presented to the emergency room with complaints of pain at his incision site along with abdominal pain. He noted his pain scale was a ten out of ten and also reported a low-grade fever. The emergency physician ordered labs and a CT scan. The labs revealed that Mr. Callaher had a slightly elevated white blood count. The emergency room physician considered infection in her differential diagnosis, examined the incision site, and noted some redness. The results of the CT scan did not provide any evidence of cellulitis or abscess. Mr. Callaher waited a total of seven hours in the emergency room. He would later learn that the emergency room staff, and the physician, made two attempts to contact Dr. Strobl's office and left messages stating that the patient was being treated in the emergency room for complaints of severe pain at the wound site. The emergency physician communicated to Dr. Strobl's office the need for the patient to be seen by Dr. Strobl. When this message was discussed with Mr. Callaher, he notified hospital staff that he had attempted to reach Dr. Strobl's office earlier that morning but had not received a return call from the physician or his staff before he felt that he needed to go to the emergency room. The emergency room physician told the patient to contact Dr. Strobl's office if he continued to have any issues and/or did not hear from Dr. Strobl's office. He was then discharged with a clinical impression of low back pain with no infection.

The following morning, Mr. Callaher's wife contacted Dr. Strobl's office to advise staff that her husband needed an appointment as he had continued pain and was vomiting. She only spoke with the front office staff and was told that he couldn't be seen that day because the office was closing early due to a practice function. She was given an appointment for two days later. Later the same day, distraught by her husband's ongoing condition and pain, the wife called the office again and finally spoke with Dr. Strobl himself. He recommended that she take Mr. Callaher to the emergency room if they couldn't wait until the appointment provided. Dr. Strobl further advised Mrs. Callaher to have the hospital staff call him if Mr. Callaher decided he needed to go there. Dr. Strobl left for the day and was out of the office for an additional day. Mr. Callaher failed to present on the day of his scheduled appointment, and no follow-up action was taken by the office staff regarding the missed appointment. Dr. Strobl would soon find out why his patient was a no show.

Unbeknownst to Dr. Strobl, Mr. Callaher presented to the emergency room hours after his wife was told he could not be seen by Dr. Strobl's office. He complained of back and flank pain giving a history of a dorsal column stimulator placement with two days of increased

pain, he had fever, was nauseous and vomiting and was evaluated by the emergency room physician. Over a two-day period and through the course of treatment, Mr. Callaher was diagnosed with a surgical wound infection and MRSA. He was also diagnosed with aspiration pneumonia, acute respiratory failure with hypoxemia, and severe sepsis. Dr. Strobl was unaware of the patient's admission to the hospital. No one contacted Dr. Strobl from the hospital despite multiple providers treating Mr. Callaher, nor did Dr. Strobl's staff contact the emergency room that was recommended to his spouse. Dr. Strobl only became aware of the admission later when his PA rounded on another patient in the hospital and learned that Mr. Callaher was there. By the time he saw Mr. Callaher, the patient had developed sepsis and was too unstable to undergo removal of the dorsal spinal column device. Ultimately, Mr. Callaher expired. The autopsy concluded that the cause of death was sepsis with the source of infection determined to be cellulitis of the lower back around the spinal cord stimulator.

Following the patient's death, his wife filed a wrongful death lawsuit. The suit was filed against our insured, Dr. Strobl, multiple providers who provided hospital care, and the hospital. Among the allegations against Dr. Strobl was abandonment. The allegations included a failure to see the patient at the hospital on the date he sent Mr. Callaher there with signs and symptoms of infection, a failure to recognize and appreciate the seriousness of Mr. Callaher's medical condition, a failure to communicate with the emergency room, the failure to make sure someone was caring for his patient, and abandonment resulting in Mr. Callaher's death.

The discovery process began with Dr. Strobl represented by a very competent defense attorney. Numerous providers were defendants to the lawsuit, which in this case added an element of difficulty in defending the claim; not only was the plaintiff's attorney alleging negligence, but other medical providers were asserting claims of negligence against each other as well given their roles in Mr. Callaher's treatment. In a case such as this, discovery depositions were very important in determining the interactions of the parties and led to some difficulty in mitigating liability as it became clear that phone calls were not answered and follow up did not occur. Physicians, staff at the hospital, plaintiff's spouse, and family friends all testified that contact was made with Dr. Strobl's office, but there was either no response or Mr. Callaher's concerns fell on deaf ears. Dr. Strobl testified that he was made aware of Mr. Callaher's initial treatment at the emergency room, but he was told that Mr. Callaher had a normal CT and that labs were not elevated so his issue appeared to be unrelated to the dorsal column stimulator. Dr. Strobl was not given any chance to handle the patient's issues in the second admission because as the saying goes, "you don't know what you don't know." The lawsuit ultimately resulted in a settlement due to the issues of lack of communication and perceived abandonment.

This case had many challenges. In a situation such as this, the medical care provided could meet or exceed the standard of care, and yet the appearance of abandonment or failure to appreciate a patient's concerns can lead to a settlement as the best resolution. Post-operative complications are always a possibility following surgery. Having a plan or protocols in place for staff to alert a physician of such complaints, missed appointments, or

a situation where complications lead to a patient's hospitalization is a must in preventing an event such as occurred in this case. In answering the earlier question of preventing a claim of abandonment, it is necessary to put protocols in place to address appropriate vacation coverage as well as staffing guidelines to tackle any problems faced when a physician is out of the office. This case illustrates the need to have advice and triage protocols for office staff as well as office procedures for when a physician is out of the office that outline the steps to take when a surgical patient calls requiring assistance. Unfortunately, we continue to see lawsuits filed by patients asserting claims of medical negligence for alleged acts of abandonment for failing to follow-up on care or delaying/failing to treat a medical condition resulting in injury.

To reiterate, the key lesson here is the need to establish guidelines to prepare for vacation, leave, and the inevitable patient calls. In developing protocols, steps should include educating and training the triage staff on how to handle calls such as documenting who, what, when, and why. If it's documented, it happened. This goes a long way in assisting in the defense of any medical malpractice claim. It's also important to ensure the provider is made aware of changes in the schedule daily. This can determine how to handle any necessary follow-up. Also, place follow-up flags on patient records as necessary. Review the chart to determine if a patient had a recent procedure to determine if complaints warrant immediate assistance. If a patient doesn't keep an appointment, contact should be made to inquire why and whether rescheduling needs to occur. Also, designate someone in the office to respond to calls if the physician is out and be sure to designate back up personnel. If possible, schedule back up physicians if the provider is out of the office. It is vital to have an outbound message for after-hours calls that provides on-call physician information, instructs a patient to go to the emergency room, or, if incident is not an emergency, to leave a detailed message. Lastly, in addressing patient messages, advise staff that calls must be returned the same day. Following such guidelines will allow for an appropriate and effective response that will help ensure patient needs are met and will likewise minimize the risk of liability from a medical malpractice claim.

[1] Medical Economics Journal, Medical Economics September 2021, Volume 98, Issue 9.

[2] Names and identifying details have been changed for confidentiality.
