Status of 2023 Medicare Payment Rate

By Elizabeth Woodcock, MBA, FACMPE, CPC

On December 29, 2022, the President signed the “Consolidated Appropriations Act, 2023” into law, sparing physicians the 4.5% payment cut to Medicare announced just weeks prior. While the decline wasn’t as bad as projected, it was far from reversed. The section, “Extension of Support for Physicians and Other Professionals in Adjusting to Medicare Payment Changes” reads:

> *“…such services furnished on or after January 1, 2023, and before January 1, 2024 [are adjusted] by 2.5 percent; and…such services furnished on or after January 1, 2024, and before January 1, 2025, [are adjusted] by 1.25 percent.”*

That’s elaborate language for stating that the cuts are 2.5% in 2023 – and 1.25% in 2024.

The newly enacted law also extended the alternative payment model (APM) incentive payment for participating physicians via the Quality Payment Program(QPP) for an additional year at a rate of 3.5%, down from 5%.

In addition to reducing the projected payment cuts, the December law addressed

telemedicine. Coverage for telemedicine is extended through the conclusion of 2024, to include the COVID-era relaxations related to patients' location and audio-only encounters. This passage is a double-edged sword for physicians; for medical practices that are offering telemedicine, the two-year extension is welcome news. However, the newly announced coverage window will continue to fuel the significant investment into virtual care ventures by private investors, in addition to well-funded public companies that are moving swiftly into the market, such as CVS, Best Buy, and Amazon. Congress stopped short of making these changes permanent, instead opting to analyze and report on the impact of telemedicine.

For more detail, click here or start on page 1439 of the new law.

New Year, New Threats- Time to Review Your Cybersecurity Program

By Rana McSpadden, FACMPE

It is a new year, and criminals are consistently coming up with new cyber threats. Now is a perfect time for practices to review and update their cybersecurity programs. Over the last two years, we have focused on providing cyber articles and resources to assist our policyholders with cybersecurity. This article serves as an amalgamation of these resources for quick and easy access.

Security Risk Analysis

In our July 2021 article, Security Risk Analysis: Step One of an Effective Cybersecurity Program, Loretta Verbeck discusses the requirement under the HIPAA Security Rule to conduct a security risk analysis. While this has been a requirement for health providers since the original Security Rule compliance date in 2005, according to the 2016-2017 HIPAA Audits Industry Report, released in December 2020, lack of a thorough and

accurate risk assessment is one of the most cited deficiencies in enforcement action taken by the U.S. Department of Health and Human Services.[1]

As with much of the Security Rule, how a covered entity conducts a risk analysis is scalable to the size and resources available to the covered entity. Complexity and technical expertise may dictate the risk analysis be outsourced to a third-party vendor that specializes in the risk analysis process. If complexity and/or technical expertise allows, an entity may choose to conduct the analysis internally. Regardless of methodology used, the entity will still need to review the final document for accuracy and completeness. To assist entities with conducting their own analysis, HHS provides guidance and tools as well as a Security Risk Assessment (SRA) Tool, which details all requirements and walks the entity through the steps of an analysis.

Security Controls

Cybercriminals do not always need to use sophisticated attacks to gain access to your systems. Lack of security hygiene allows weaknesses in systems that cybercriminals exploit to gain easy access. In his October 2021 article, Cyber Attack Prevention Strategies, Brian Johnson defines security hygiene as “basic and fundamental security practices that must be in place to properly secure your environment”.[2] Password use alone cannot thwart cybercriminals as they have many tactics to obtain passwords. Complex password requirements, such as utilizing upper case, lower case, numbers, and symbols in a password, may still lead to easily guessed passwords because users too often create passwords which are easy to remember. Cybercriminals may also purchase breached passwords through the Dark Web. With much of the population being creatures of habit, many users will reuse the same password for multiple sites. If one of those sites is compromised, cybercriminals potentially have access to every other account for which the individual has reused the same password. Cybercriminals may also employ social engineering to trick a user into disclosing their password by use of “sending a phishing email, impersonating a trusted person, company, or brand, containing a link to a very realistic, but fake, login screen. Once the victim’s password is entered on the bogus login screen, the cybercriminals are well on their way to compromising your network.”[3]

Mr. Johnson continues in his article by discussing various solutions to password security weakness. One of those tools is utilizing Multi Factor Authentication (MFA), which adds a second layer of authentication in addition to a password. MFA may be a text sent to a trusted device or through a push notification through an app. Mr. Johnson also goes on to discuss the risks of running outdated and unpatched software and recommends establishing a patch maintenance program to ensure the most recent and secure operating system is running on all computers and devices.

Data Backup

Imagine coming into your practice one morning and no longer having access to your medical records. Maybe the server crashed over the weekend, cybercriminals took over your systems through ransomware, or there was a fire or flood that destroyed the computers. Utilizing good data backups, systems could potentially be back up and running with hopefully minimal to no data loss. In his August 2021 article, Back It Up- The Importance of Proper System Backups, Brian Johnson focuses on the Security Rule's requirement that covered entities maintain the availability of electronic protected health information (e-PHI) through the use of data backups.

Mr. Johnson defines backups as "duplicate copies of the critical data that run your practice" and "are a core component of any Business Continuity plan…"[4] Entities must consider all systems that contain this critical data, not just the electronic health record (her). Lab systems, PACS for imaging, patient photos, and financial files are all data systems that should be considered for backup. In addition to deciding what to backup, entities should also consider how each piece of data should be backed up as some systems will require different solutions, and where to back up the data; media type (disk or tape) and physical location (cloud or onsite). Finally, consider how often each piece of data should be backed up. This schedule will be determined by the rate at which the data changes and how much data you are willing to lose. While a much tighter backup schedule may be required for data that changes often, or if the amount of data you are willing to lose is limited, a less restrictive schedule may be better for if your data changes less frequently or is not as critical to lose.

Educating and Testing Staff

Much like the HIPAA Privacy Rule requires workforce member training on privacy, the Security Rule requires entities to train their staff in the risks associated with cybersecurity. Rana McSpadden describes the process of creating an education program in her April 2022 article Cyber Education is More Than a Meeting. When creating an education program, entities should identify which staff members need education, how often to provide this education, what topics to include, and how to provide education.

Topics to consider including in a cyber education program include password management, risks associated with phishing, ransomware, and social engineering. Two articles, Don't Take the Bait in 2021 and Ransomware 2.0- The New Generation of Ransomware provide information entities can use in their education programs on phishing email and ransomware. Phishing emails "impersonate brands, companies, people, and processes you trust. Next, they play on emotional triggers that manipulate your social tendencies that include authority, urgency, fear, duty, and a desire to be helpful."[5] Staff should be educated on how to spot these and what to do if they receive one. In addition to providing education on phishing, entities may also choose to test their employee's ability to spot a phishing email. Many vendors offer a free trial; one such entity is KnowB4 who offers a free test to entities interested in starting a testing program.

Phishing is not just a threat through email, as we discussed in our October 2022 article Phishing by Fax: Do Not Become a Victim. Similar to phishing emails, criminals impersonate legitimate entities through other means, such as fax, mail, text, or phone calls. It is important to be suspicious of any unsolicited request for confidential information and scrutinize the request for any red flags that it may be a phishing attempt.

Ransomware is a type of malware that, once deposited into the system, can live undetected for an undetermined amount of time until cybercriminals initiate the attack to overtake the system and hold it for ransom. In recent years, ransomware attacks have evolved into not only holding the system hostage, but also exfiltrating the data and selling it on the Dark Web unless their ransom demands are met. [6]

Incident Plan and Response

Inevitably, regardless of the safeguards in place to prevent security incidents, an entity will more than likely experience some sort of incident potentially impacting its data or information system. Justin Joy outlines what a security incident is, how to respond to an incident, and how to develop an incident response policy in his November 2021 article, Obligations of Medical Practices in Responding to Data Security Incidents (Not Just Data Breaches). He defines the difference of an incident and a breach as:

- a security incident is "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."[7]
- a breach is defined as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information."[8]

While every breach is considered an incident, not every incident is considered a breach. Entities are required to have an incident response plan to address how to respond in the event a security incident takes place, whether it is considered a breach or not. Steps to consider when developing that plan include:

- The plan needs to provide the specific definition of a security incident, which should be based in substantive part—if not verbatim—on the definition found in the HIPAA Security Rule.
- The plan may also specify types of events that do not require an immediate investigation response because of their minimal or nonexistent risk.
- The plan also needs to identify the individual, who can be the HIPAA security and/or privacy officer, within the organization that workforce members should notify upon discovery of a security incident.
- Relatedly, the plan document should also identify the members, either by position (such as IT, HR, marketing/PR and legal counsel) or by name with contact information, of a team or committee of individuals who will be activated in the event a response is required. External resources, such as SVMIC, should also be included in the plan.
- Finally, requirements related to documentation should be included as well, perhaps providing sample reporting forms upon which the information to be collected about the event is to be provided.[9]

In Closing

There are many components to any cybersecurity program. How an entity approaches their program may help in reducing the risks of a cyber-attack. SVMIC provides many resources to assist our policyholders with developing their program as well as providing educational resources for their staff. We have recently developed a Cybersecurity Essentials resource for quick access to many of our cyber resources we have developed over the last two years. A full list of cyber resources can be found here. For access to any of our previous cyber articles, they can be found here.

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 SVMIC as soon as possible by calling 800-342-2239 and ask to speak with 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.

[1] 2016-2017 HIPAA Audits Industry Report

[2] Cyber Attack Prevention Strategies

[3] Cyber Attack Prevention Strategies

[4] Back It Up- The Importance of Proper System Backups

[5] Don’t Take the Bait in 2021

[6] Ransomware 2.0- The New Generation of Ransomware

[7] 45 C.F.R. § 164.304.

[8] 45 C.F.R. § 164.402.

[9] Obligations of Medical Practices in Responding to Data Security Incidents (Not Just Data Breaches)

QPP Application for Exemption Extended

By Elizabeth Woodcock, MBA, FACMPE, CPC

The deadline to submit your 2022 Quality Payment Program data is March 3, 2023, at 8 pm EST.

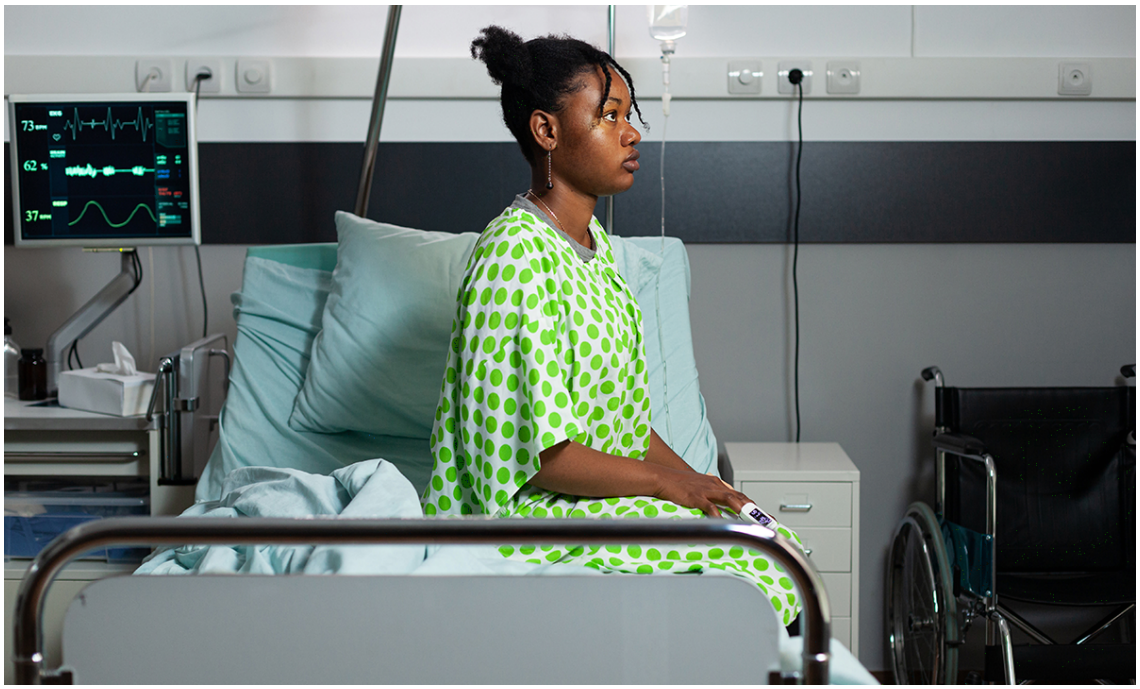
If you are required to participate in the Quality Payment Program (QPP) based on your volume of Medicare payments or patients, submit your data for 2022. For medical practices that do not have sufficient data to submit for its flagship program, the Merit-based Incentive Payment System (MIPS) – or your data will fall short of the minimum reporting threshold, don't despair. The federal government just announced an extension of the hardship exception application. If COVID disrupted your practice in 2022, you can opt out of the program (and its daunting 9% penalty, applied to all Medicare reimbursement in 2024) altogether. No proof of disruption is required, and the application takes only minutes. The deadline is March 3, 2023, at 8 pm EST. Note that if any data is submitted, it will override your Exemption qualification. Find the application – and more information – here.

Risk Matters: The Unintended Mistake

By Jeffrey A. Woods, JD

Wrong-site, wrong-procedure, wrong-patient errors (WSPEs) continue to occur at an unreasonably high frequency as reflected in our reported claims. This is especially true for spinal surgeries. The causes can often be traced back to nonadherence to the Universal Protocol, erroneous site markings, and/or failure to perform a “timeout” or checklist. Some providers apparently believe, “this would never happen to me,” or “I would never make such an error.” Unfortunately, they often discover that anyone can find themselves the target of a malpractice claim as a result of this type of mistake, and as pointed out in an earlier article, few medical errors are as indefensible as WSPEs.

A Case of Retrospective Clarity



By Jamie Wyatt, JD

There is not a day that goes by without an emergency or some type of accident. These scenarios are what make emergency medicine necessary. The American College of Emergency Physicians defines emergency medicine as “the medical specialty dedicated to the diagnosis and treatment of unforeseen illness and injury…[e]mergency medicine encompasses planning, oversight, and medical direction for community emergency medical response, medical control, and disaster preparedness.”[1] The fast-paced nature of emergency medicine forces emergency physicians to make quick decisions and take decisive action based on limited information in order to do what is best for a patient they’ve just met.” These challenges inherently increase liability. In fact, 1 out of every 14 emergency physicians get sued each year. [2] How can liability be reduced? Our claim review touches on the pitfalls of practicing medicine in this environment and the important role thorough documentation can play in combating potential liability.

This claim involves the treatment of a 20-year-old female, Amelia Thomas[3], who presented to the emergency department via EMS. EMS was called when it was reported that emergency services were needed to treat a young woman who was exhibiting

abnormal behavior at a party. The EMS notes were an important aspect of the case as an EMS responder documented that the patient was compliant with care and assisted EMS with her treatment. Documentation noted that the patient remained alert, but non-verbal during transport. All four of the patient's extremities were evaluated for strength and abnormal movement, and no abnormalities were found. Particularly due to the drug paraphernalia found at the scene, an initial diagnosis of drug intoxication was given. When the patient presented to the emergency department Dr. Strobl, our insured emergency physician, provided care. He documented that the patient was uncooperative. He specifically noted that the patient was able to move all her extremities. Most importantly, he noted that her neurological exam was limited due to Amelia's lack of cooperation. Her musculoskeletal assessment was within normal range for motion and strength. Dr. Strobl observed the patient giving nonverbal answers to questions asked. She would shake her head yes or no. Labs were taken, and the urine drug screen was positive for marijuana. A chest x-ray was negative for an acute cardiopulmonary process. The patient was discharged later that night. On discharge, Dr. Strobl documented that the patient's mental status had improved, and that Amelia's condition was unchanged. The thought was that Amelia's symptoms were the result of recreational drug use. The discharge diagnosis was marijuana use, with a differential diagnosis of confusion, alcohol intoxication, and drug abuse.

A few days following discharge, Amelia's mother called EMS due to her daughter's altered mental status. She stated to EMS that her daughter was recently sent home from the hospital with the same signs and symptoms (altered mental status and inability to ambulate) as they were presently seeing. EMS noted that the patient was able to move her left side and while she was trying to speak, nothing came out. The patient was awake and alert, but non-verbal initially. This eventually improved in transport, and Amelia became verbally responsive while in the ambulance. She responded to her name and advised that she did not know the answers to the other questions used to assess her orientation. Her speech was slurred. It was unknown how long this had been occurring because she had been non-verbal around her family. EMS noted that the patient had slurred speech and right-sided weakness for the past 48 hours.

She was seen by an ER physician. His neurological exam revealed that her right side was flaccid, her speech was slurred, and she was disoriented. She appeared moderately confused, but she answered some questions appropriately. Her ROM of her right side was limited. She admitted to smoking "weed." A CT scan revealed a significant abnormality (stroke vs. mass). The impression of the CT scan report was that her findings could represent vasogenic edema secondary to underlying parenchymal brain lesions with etiologies including brain ischemia or an infarction.

Amelia was then transferred to another facility. Her H & P noted that she was aphasic. This time when she was asked questions, she had a challenging time differentiating between yes and no. She also had difficulty understanding and following simple commands. An exam revealed dense right facial paralysis, and she was not able to understand the instruction to stick out her tongue. She had dense right flaccid hemiplegia,

but she seemed to have sensory perception on the right because she grimaced when her right lower extremity was touched. An MRI showed that the patient had a large acute left MCA territory infarct and moderate surrounding edema. Findings of a transthoracic echocardiogram found that the patient had a mitral valve echogenic shadow that was suspicious for vegetation. Neurology noted right hemiparesis, aphasia, and hypersomnolence. Amelia underwent another CT scan, which revealed that she had suffered a left middle cerebral artery stroke. Cardiology was consulted and included a differential diagnosis of endocarditis versus a mass that was likely due to stroke. Amelia remained an inpatient for three weeks and then went on to rehab.

A lawsuit was filed by the patient, alleging that the care provided by Dr. Strobl, his practice, and the hospital did not comply with the standard of care. The primary allegations against Dr. Strobl were failure to timely recognize symptoms of a stroke; failure to perform a stroke assessment; failure to timely perform a neurological exam; failure to obtain a CT scan; failure to timely administer treatment for acute ischemic stroke; and discharging Amelia Thomas in an unstable condition.

The alleged damages were high in this suit because the patient sought compensation for her disfigurement, loss of capacity for the enjoyment of life, pain and suffering, medical expenses, loss of earning capacity, lost wages, and mental anguish. The amount of economic damages alone were especially high given the young age of the patient and a long life expectancy, the expensive life care plan, and the permanent injury she sustained. The monetary demands from the patient's attorney removed the possibility of settling the matter as they were well over the amount of Dr. Strobl's policy limits.

The case had many hurdles from a defensibility perspective.

The first was the perception of an unintentional or unconscious bias as a result of the patient presenting as a drug user which the plaintiff argued had an impact on the care provided by our insured physician. This was an easy argument to make given, at first glance, this case could appear to demonstrate a physician who failed to thoroughly investigate symptoms relative to a stroke in a young person as it is an uncommon event, and assumed it was due to drug intoxication because of the presence of drugs in her urinalysis and the EMS record. This narrative was the first thing argued to the jury in opening statements. Plaintiff's counsel pushed the idea that our physician was very busy, and he assumed the patient was a drug addict, so he put little effort into investigating the cause of the symptoms, basing his diagnosis on the obvious choice of drug intoxication as the cause of her condition.

Another big hurdle was inconsistencies in the records due to the overall lack of documentation. Documentation from EMS stated that the patient was awake and compliant. She was trying to assist EMS but was non-verbal. Dr. Strobl admitted he failed to change the template default for documentation in his H & P, which described the patient as cooperative with normal judgment. It wasn't until Dr. Strobl testified during the trial that he specifically recalled she was noncompliant by pulling off the monitor leads and pushing the nurses' hands away. This was also consistent with the nurses' testimony. This missing

language, if it had been noted in the record, would have gone a long way in explaining that Amelia could move her extremities when Dr. Strobl examined her and would have supported his drug intoxication diagnosis. Documentation helps support the veracity of testimony, leaving little doubt for a jury. He testified that, as he documented, her musculoskeletal assessment was normal.

Another point that the patient's attorney used against Dr. Strobl was the incomplete neurological exam. The medical record documented that neurological exam was limited due to the patient's lack of cooperation. He testified that he observed Amelia Thomas making fists but did not document this. In his testimony, he agreed that the inability to move one side of the body can be a stroke sign, but this is not something that he saw when the patient was in the ER. Dr. Strobl asserted that the patient appeared to be choosing when to respond and that her presentation appeared to be more of a refusal to speak than an indication that she could not speak.

Lastly, documentation was an issue in refuting the allegation of discharging an unstable patient. On this point, the plaintiff's attorney questioned the mother on the stand about her allegation that she had to physically drag her daughter out of the ER. She testified that the patient was unable to walk and was in the same condition as she was when she presented. Dr. Strobl re-examined the patient before discharge. However, his note was short and noted only that the patient's condition was unchanged, but with mental status improvement. No elaboration was made, and there was no documentation as to what he observed or their interaction. Again, Dr. Strobl's testimony was needed to make clear that Amelia Thomas was answering yes and no questions with a clear speech pattern. If he had elaborated on his note indicating that the patient was not speaking before and then began speaking at discharge, this information would have been helpful when defending the alleged failure to diagnose a stroke. Additionally, Dr. Strobl did not document his interaction with Amelia's mother. He testified that, at discharge, she agreed that her daughter was improving and signed the discharge instructions. This testimony painted a very different picture than what was presented by the medical records alone. The testimonial inconsistencies along with the scant documentation made the case challenging to defend because it created a "he said/she said" scenario and forced the parties' credibility to come into question.

Despite these hurdles, Dr. Strobl's presentation on the stand, and his credibility, helped his defense. He was able to fully explain his clinical thought process and observations, filling in the gaps his documentation left at the time of treatment. Without Dr. Strobl's persuasive testimony at trial, along with the skills of his talented counsel, this case could have been lost. Fortunately for Dr. Strobl, the jury found that there was no breach in the standard of care and rendered a defense verdict.

By its nature, emergency medicine calls for fast paced care and quick cognitive agility. Even though time may be short, documenting clinical observations and analysis ensures retrospective clarity. Perhaps with more thorough documentation on the front end, this lawsuit may not have been filed.

Some best practice takeaways:

Translate clinical thoughts and observations to the record that paint a picture of the patient's condition so you can clarify medical decision making. Although you may have time pressures, it benefits you to document well. Any change in the patient's treatment or additional information provided by family or friends should be included.

Be aware of EHR templates. Make sure findings make sense in the context of the visit. Check for inconsistencies.

Consider a re-examination of a patient at discharge. When preparing a discharge summary, it is helpful to be specific in diagnosis and observations. Include relevant information provided by a family member.

[1] American College of Emergency Physicians. Jan. 2021.Definition of Emergency Medicine. Retrieved from http://www.acep.org/patient-care/policy-statements/definition-of-emergency-medicine

[2] Aya Itani, MD, MPH; Cedric Dark, MD, MPH, FACEP. Emergency Medicine Advocacy Handbook. Retrieved from http://www.emra.org/books/advocacy-handbook/liability-reform/

[3] The name of the physician and patient information have been altered.