MIPS Penalty Exemption Applied to All Clinicians

By Elizabeth Woodcock, MBA, FACMPE, CPC

On February 25, 2021, the Centers for Medicare & Medicaid Services (CMS) declared that a hardship exception would retroactively apply to all eligible clinicians for the 2020 performance year of the Quality Payment Program (QPP). The announcement, which came just weeks after the deadline for the exemption application had passed, was certainly welcome news. Eligible clinicians – physicians and advanced practice providers – were facing a whopping 9% penalty in 2022 for failure to participate successfully in the program. This was a particularly painful cut following the challenges of 2020 brought on by the pandemic, coupled with the Medicare reimbursement cuts imposed for 2021.

Although you have until the end of the month – March 31, 2021 at 8 pm EST, to be exact – to report your 2020 data via the Merit-based Incentive Payment System (MIPS) or an Advanced Alternative Payment Model (AAPM), **you will not be penalized should you fail to do so. Indeed, you will automatically be identified to receive a neutral payment adjustment in 2022.**

If you already reported – or you are planning to report - the exception will not be applied. According to CMS, it cannot be used to override data that you submitted previously under MIPS. Eligible clinicians who submit data will be scored and receive a bonus in 2022, as applicable. The QPP was established as a program in which the penalties are transferred to successful participants in the form of payment boosts. Because there will be no longer be “losers” in 2020, however, there will be less funds to distribute to the “winners.” Fortunately, there is still money left in the coffers that Congress set aside for exceptional performers. These funds, which were appropriated for the first five years of the program, will be used for the 2022 distribution to eligible clinicians who exceed the performance threshold.

The previous three years have seen increases of less than two percent even for the highest performers; given the circumstances, this trend will most likely continue.

Should you wish to report, click here for more details on how to report:
https://qpp.cms.gov/login

Little Things Make Big Things Happen

By J. Baugh, JD, CPA

> *"It's the little details that are vital. Little things make big things happen." - John Wooden*
>
> *"In the successful organization, no detail is too small to escape close attention." - Lou Holtz*

These quotes are from two men who had very successful careers. John Wooden won 10 national championships as UCLA's men's basketball coach in the 1960's and 1970's, and Lou Holtz won a national championship as Notre Dame's football coach in 1988. Both men are known not only for their successful coaching careers, but also for their words of wisdom during and after their careers of coaching collegiate athletes. These quotes about the importance of details apply to sports and to life in general. They also apply to the practice of medicine, as you will see in the case below.

A 38-year-old female patient with a history of abnormal pap smears was seen by Dr. Ben Garrett, an OB/GYN, to undergo a colposcopy. Prior to the procedure, a nurse prepared a tray with the necessary solutions, biopsy containers, and tools. One of the containers on the tray had cotton balls which should have been soaked in a very light acidic solution consisting of 50% vinegar and 50% sterile water. However, the nurse mistakenly soaked the cotton balls in trichloroacetic acid (“TCA”). She mistook the large gallon jug of TCA for a gallon jug of premixed vinegar/sterile water solution. TCA is highly corrosive and is used by Dr. Garrett to burn genital warts.

The nurse took the tray to the exam room for Dr. Garrett to use in the examination. Dr. Garrett placed the soaked cotton balls inside the patient’s vagina to detect any possible lesions. The cotton balls typically stay in place for 3 to 5 minutes. Unfortunately, Dr. Garrett had a bad cold, which inhibited his ability to smell. Had he not been experiencing a cold at the time, it is possible (maybe likely) that he would have appreciated the fact that the nurse had not used the vinegar/sterile water solution given the absence of the distinctive smell of vinegar.

Shortly thereafter, a medical office assistant walked by the patient’s exam room and noticed the patient was in pain. The patient said she was hurting and burning. The medical office assistant told the patient that some burning is normal because vinegar is an acid, but she noticed the patient was in more pain than normal. The medical office assistant told Dr. Garrett about the unusual level of the patient’s pain. Dr. Garrett examined the patient and determined the cotton balls had been soaked in TCA rather than in the vinegar/sterile water solution. Dr. Garrett flushed the patient’s vagina with copious amounts of water and applied K-Y jelly to her skin. He prescribed Premarin vaginal cream twice per day and asked that she return to see him in 3 days. For the next 10 months, the patient was treated with creams, physical therapy, a Tens unit, a nerve block, and steroid injections.

A lawsuit was filed against Dr. Garrett, the medical office assistant, and the hospital that employed the nurse who prepared the colposcopy tray. (It is unknown why the patient did not also name the nurse as a defendant in the lawsuit.) As of the time of the filing of the lawsuit, the patient continued to complain of pain, bleeding, depression, and the inability to have intercourse.

The nurse who prepared the colposcopy tray started working in Dr. Garrett's office just 5 days before this incident. She had previously worked for Dr. Mike Walker, another OB/GYN, for 3 years. She was very familiar with the colposcopy procedure because Dr. Walker also regularly performed colposcopies. Dr. Walker also soaked the cotton balls in a vinegar/sterile water solution. However, the solution used in Dr. Walker's office was in a premixed container labeled "Acetic Acid Solution" and was similar in size and color to the TCA container used in Dr. Garrett's office. Also, Dr. Walker did not use TCA in his practice, instead using CO2 to cryogenically burn genital warts. Unfortunately, the nurse thought the bottle of TCA in Dr. Garrett's office was the type of premixed vinegar/sterile water solution that was used in Dr. Walker's office. She saw the word "acid" and assumed it was the acetic acid solution. She didn't know that Dr. Garrett's staff mixed their own solution and stored it in a gallon water jug. This was the first time the nurse had ever used TCA.

The details that were overlooked in this case caused the wrong solution to be used during the colposcopy and made the overall defense of this case almost impossible. The nurse assumed the TCA container in Dr. Garrett's office contained the same type of vinegar/sterile water solution that was in the container labeled "Acetic Acid Solution" in Dr. Walker's office. Another detail that was discovered by defense counsel after the lawsuit was filed is the fact that the nurse added handwriting to the label on the container of soaked cotton balls that said "Trichloroacetic acid." The nurse had never used TCA, but if Dr. Garrett had read the label on the cotton ball container, he would have known that they had been soaked in TCA rather than in a vinegar/sterile water solution. While it could be argued that Dr. Garrett should be able to rely upon the nurse to perform her duties appropriately and within the standard of care, a jury might reach the conclusion that Dr. Garrett should have taken the time to read the label that the nurse created and ensure that the cotton balls had been properly prepared. Another reason this case would have been difficult to defend is the type of injury that the patient experienced. The patient's medical bills over the 10+ months of treatment were significant, and juries have awarded high amounts for pain and suffering for injuries to sensitive areas of the body in the past. Because of the difficulty in defending the care at issue in the case, the type of injury the patient experienced, and the extended medical treatment that was required because of the injury, SVMIC and the hospital entered into a joint resolution of this case.

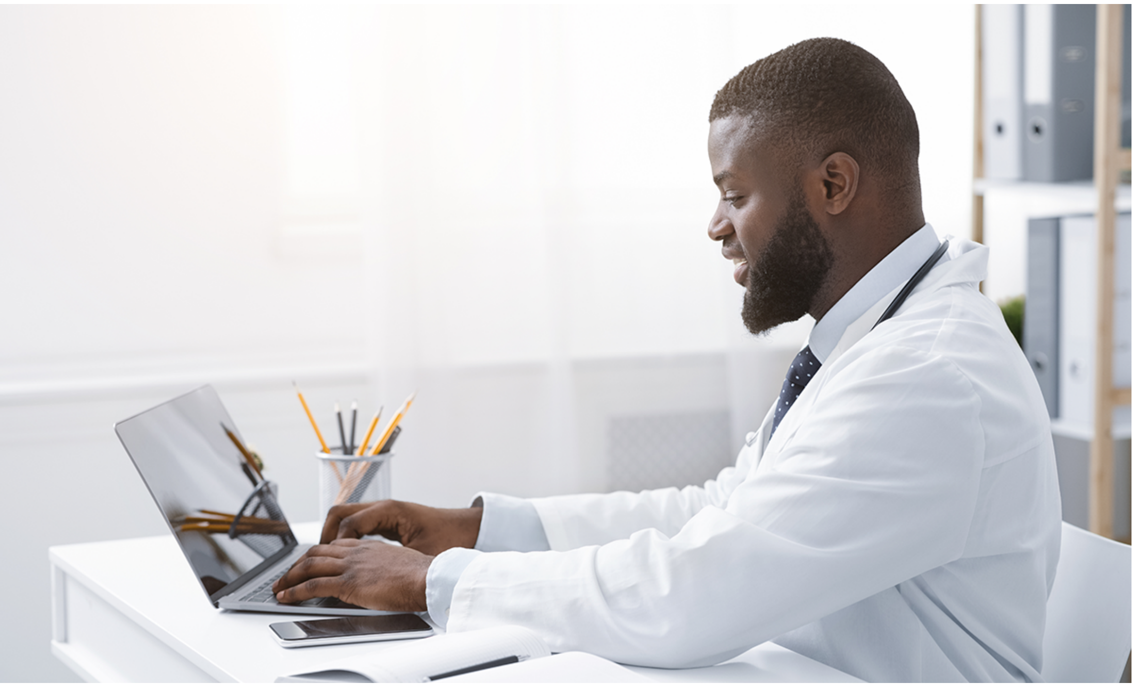
As was mentioned at the beginning of this article, details can be very important in many situations, and that would include the treatment of patients. While it is understandable that medical practices are very busy, it is always a good practice to remember the importance of noticing and acting upon each detail in providing medical treatment to a patient.

Risk Matters: Informed Consent

By Jeffrey A. Woods, JD

Informed consent is often the most important discussion that physicians will have with their patients, but unfortunately, it is sometimes viewed as merely obtaining a signature on a pre-printed form. While lack of informed consent is rarely the central issue in a malpractice lawsuit, it is almost always included as an additional allegation. For this reason, it is important to keep in mind that, while the physician may be assisted by other healthcare professionals in providing consent-relevant patient education and/or obtaining a signature on the consent form, the **individual who actually renders the care is legally and ethically responsible** for providing the information upon which the consent is obtained. What does this mean? When a lack of informed consent claim is alleged, it will typically be asserted against the physician and *not* the nurse or non-physician staff who obtained the signature on the form. From a risk management perspective, the informed consent process plays a vital role in minimizing exposure to medical negligence lawsuits because it involves patients in their medical treatment and helps keep expectations realistic.

Microsoft Vulnerability Highlights Steps We All Need to Take



By Brian Johnson

A recently discovered vulnerability[1] in Microsoft's popular Exchange email server puts companies using this application at extreme risk. Security researchers have dubbed this event Hafnium, named after the Chinese-based espionage group first seen attacking servers. Once compromised, multiple backdoors[2] are installed on systems that will likely lead to complete takeover of hacked systems. As of March 5th, over 30,000 U.S.-based companies were known to be compromised. If you are running a Microsoft Exchange server[3], hopefully you have addressed this issue; if not, you need to act now and install emergency patches[4] provided by Microsoft. Security researchers at UNIT221B have put together several resources that include links to patches, methods to test your server, and resources to restore a compromised server. Investigative reporter, Brian Krebs, has a detailed article on the issue at KrebsonSecurity.com.

Major security events such as this are a reminder to evaluate your own security practices and prepare for the next big event. This incident demonstrates how fast cybercriminal groups will pounce on the opportunity to exploit vulnerable systems, so it is a good time to highlight security practices that can help defend against future threats.

The Hafnium incident demonstrates the classic cat-and-mouse game between cybercriminals and software vendors. Cybercriminals discover a vulnerability that can be exploited, and the software vendor releases a security patch to fix the issue. Unfortunately, releasing a patch broadly publicizes the existence of the vulnerability. Cybercriminals then race to exploit the weakness before the patch is fully deployed[5]. As a result, this leaves a small window for organizations to patch systems before cybercriminals can attack. Companies that develop routine procedures to patch and update systems will fare better in these situations. **It is important to know your systems and applications and how each is updated.** Microsoft, for example, releases patches for Windows and Office the second Tuesday of every month, a day known as “Patch Tuesday.” This process can be automated, ensuring that systems are fully patched and protected. Some applications, such as Chrome and Edge browsers, can also be configured to auto update. Other applications may require a manual download and install of the patch, as was the case to patch Exchange servers against Hafnium. Now is the time to inventory your systems and applications, learn how they are patched, automate where possible, and implement routine procedures.

Backups[6] are a safety net that can help save the day and restore a compromised system back to normal operation after a security event. Consider a ransomware[7] scenario where cybercriminals encrypt and hold your data captive until a monetary payment, usually in Bitcoin[8], is made. A good backup allows you to forego the ransom payment and restore your systems back to normal. Like the patching process, every software application has a different backup method. **It is important to understand your application, what data you are backing up, and how to restore it.**   Additionally, test your backups periodically to ensure that you are correctly saving the data and it can be restored to a usable state. Store your backups in a safe place, preferably on removable media or in the cloud away from your network. If cybercriminals can compromise your network and install ransomware, they will have enough access to find and destroy your backups, increasing the odds that you will pay the ransom.

A good security strategy includes an incident response plan. At a minimum, **know who you are going to call after a security event.** You will need a skilled security expert to perform a forensic investigation[9], clean your systems, and ensure the holes are plugged. If your incident involves the disclosure of protected information such as health or financial records, you will be required to notify the victims and the government and possibly provide identity and credit monitoring services.

If you encounter a security incident, contact SVMIC immediately to start the mitigation process. Your cyber liability insurance policy will provide the necessary resources and cover the cost of recovery within the limits of your policy. Additionally, SVMIC members can access much more information regarding cyber risk assessment and prevention at vantage.svmic.com.

[1] Hole or a weakness in the application, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application

[2] Feature or defect of a computer system that allows surreptitious unauthorized access to data

[3] Mail *server* and calendaring *server* developed by *Microsoft*.

[4] Set of changes to a computer program or its supporting data designed to update, fix, or improve it.

[5] Software tool designed to take advantage of a flaw in a computer system, typically for malicious purposes such as installing malware.

[6] Copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event.

[7] Type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

[8] Cryptocurrency invented in 2008 which began use in 2009; currently (March 2021), 1 Bitcoin = approximately $57,300 USD.

[9] Gathering and analysis of all related physical evidence in order to come to a conclusion.

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.