Patient Payment Plans: Seven Tips for Success

By Elizabeth Woodcock, MBA, FACMPE, CPC

Payment plans permit the patient to pay off the amount they owe for a service over a period, instead of requiring a lump sum payment. Offering payment plans to patients benefits your practice – and your patients; however, execution is key. Consider these tactics for success:

1. Put the ball in the patient's court: instead of leading with the parameters of the plan, ask the patient, "How much more time do you need?"
2. Set a minimum payment; for example, $25, and maximum duration such as 12 months.
3. Keep it simple by seeking the "odd" payment upfront – for example, if $231.53 is owed, collect $31.53 at the outset, followed by eight $25 payments due.
4. Always collect the initial installment upfront; don't set up a plan – and then let the patient walk away without paying anything.
5. Automate the process of reviewing for non-compliance: set your system to push the

accounts with two missed payments to a work queue and have a rigorous protocol for follow-up.

6. Integrate your plan with a text-to-pay option or collect a credit card upfront. (Be sure to follow federal and state laws regarding storing credit card information.)
7. Establish an insurance category for payment plans, which is separate from patient receivables; this distinction allows for better reporting, as your practice has agreed to maintain the balance on your accounts receivable.

Payment plans may ease the challenges faced by practices based on incurring bad debt. Patients bear a greater financial responsibility than ever before. It is an opportune time to offer payment plans for patients, but execution is essential for medical practices.

Risk Matters: Obstetrics Risks

By Jeffrey A. Woods, JD

Obstetrics is a very rewarding field of medicine that celebrates the beginning of life and the joy of parenthood, but it's also a field fraught with complex challenges and, at times, devastating outcomes. At its best, obstetrics exemplifies the compassion, expertise, and dedication of healthcare professionals. However, like any area of medicine, it is not without risks. One of the most distressing and heart-wrenching events for an obstetrician is the impairment or death of a newborn. While this can and does occur without medical error, when negligence is involved, it poses a significant challenge for the practitioner and the defense.

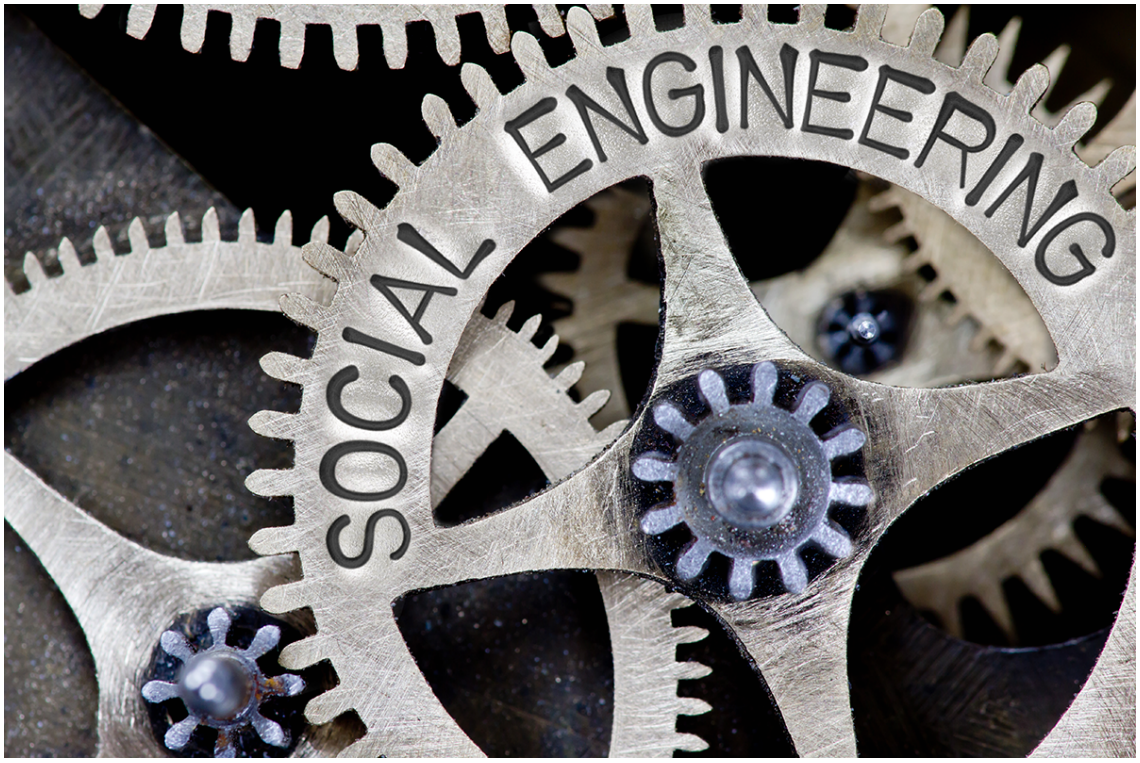
SVMIC has added a new obstetrics program entitled, "**Obstetrics – Lessons from a Defense Attorney's View,**" to our online courses. The purpose of this program is to discuss a difficult and crucial issue: medical malpractice in obstetrics. The program delves into the complexities, seeking to understand some of the most common causes, consequences, and most importantly, solutions that will not only improve patient safety,

but reduce the likelihood of a malpractice claim or lawsuit.

Our speaker, Mr. Tom Wiseman, is an experienced defense attorney who has practiced law for over 35 years. His practice focuses on medical malpractice defense, including the defense of birth injuries during labor and delivery. In this course, Mr. Wiseman discusses the primary obstacles he has encountered that can affect the successful defense of an obstetrics malpractice case from a defense attorney's perspective and, specifically, the key areas that will likely be the focus at trial.

For more information, please contact us at ContactSVMIC@svmic.com.

Social Engineering Took Down Giants. Don’t Let It Take You Down, too.



By Rana McSpadden, FACMPE

In September 2023, MGM Resorts International and Caesars Entertainment reported they were victims of a cyberattack. The attack disrupted operations for multiple MGM properties for an extended period of time and ultimately cost the company an estimated $100 million [1]. Caesars Entertainment paid $15 million of the hackers' original $30 million demand to avoid system disruption. In these attacks, hackers stole customers' personal information, such as names, Social Security numbers, and driver's license numbers. These companies take security seriously, so how did hackers access their systems in the first place? They did it through social engineering. There are numerous social engineering tactics but here hackers used information gleaned from LinkedIn to impersonate company employees, call the IT helpdesk, and trick them into providing system access[2].

Would this tactic work in healthcare? It already has. On January 12, 2024, the American

Hospital Association (AHA) reported on a "validated IT help desk social engineering scheme that uses the stolen identity of revenue cycle employees or employees in other sensitive financial roles." [3] Much like the cyberattacks on MGM and Caesars, hackers impersonated hospital employees to trick IT staff into providing user login information. They had enough information on the employee to provide answers to security questions. Once the helpdesk confirmed this information, the hacker would ask to change the password and register a new device, such as a cell phone. By doing so, the new device could be used to bypass multi-factor authentication (MFA). After the hacker gained access to the employee's email and login, they would change payment instructions for their payment processors and have funds redirected to a fraudulent bank account.

Regardless of how basic or sophisticated the cybersecurity program a practice has in place to prevent a cyberattack, social engineering bypasses all of this by exploiting the human factor. There is no way to 100% prevent a cyberattack caused by social engineering, but practices can certainly reduce the risk by educating staff on what to watch for with different types of social engineering.

Types of Social Engineering

The most common form of social engineering is phishing. Hackers send victims fraudulent communication, impersonating legitimate individuals or organizations to collect sensitive information, such as passwords and other personal data[4]. Because the communication looks like it comes from a legitimate source, links embedded in the communication take victims to fake websites used to , download malware or collect login information and other personal data. Email is the most common form of phishing. Some signs to watch for include poor grammar, odd-looking URLs, and requests for personal information[4]. However, hackers are increasingly utilizing generative AI technology, such as ChatGPT, so some warning signs of phishing emails, such as spelling mistakes or poor grammar, are becoming less common.

Phishing by phone, or vishing, is another form of phishing. This is the form of phishing used by the hackers of MGM, Caesars, and the hospital noted by the AHA article referenced earlier. With vishing, hackers call into an organization and impersonate an employee, IT provider, or other vendor to gain login information or access to the system. Once hackers gain access, they can steal information and/or load malware or ransomware into the system for further exploitation. To prevent vishing, be cautious of unsolicited calls, especially from vendors. Confirm the caller's identity by calling the number the practice has on file for the individual (if claiming to be an employee) or company (if claiming to be a vendor). Caller ID isn't always trustworthy, as scammers can spoof caller ID to show a legitimate number[5], which is why it is essential to call the number on file rather than rely on caller ID.

Smishing, or phishing by text, is the third form of phishing. Like phishing by email, victims are sent a text, generally with a link to a fraudulent website, to collect personal information, or download malware to the device. Texts may claim to be from a bank, credit card, or delivery service, such as USPS[6]. If this sort of text is received, avoid clicking any links

and call financial institutions using the phone number on the back of your credit or bank card rather than using any phone number included in the text.

Phishing and the Office for Civil Rights

Patient data breaches from phishing cyberattacks can result in financial penalties imposed by the government. On December 7, 2023, the Office for Civil Rights (OCR) announced its first settlement of a breach caused by a phishing attack[7]. Lafourche Medical Group of Louisiana notified the OCR on May 28, 2021, of a breach of 34,862 individuals' protected health information when hackers using a phishing attack accessed an employee's email account containing protected health information. The settlement requires Lafourche Medical Group to pay the OCR $480,000 and go under a corrective action plan for two years.

Closing Thoughts

Whether your group is large or small, social engineering and phishing are a threat. Utilizing the services of professional and qualified IT vendors or staff is important. Often, they can customize a cyber program to meet the budget needs of a practice. Educating staff on what to watch for and their responsibilities to prevent cyberattacks is vital as well. SVMIC has a new Compliance Center, which includes new cybersecurity education, along with other useful compliance tools. Additionally, consider testing staff on their ability to spot a phishing email. Companies such as KnowBe4 have testing resources (sometimes free) available.

With the ever-increasing risk of a cyber-attack, it has become a best practice for organizations to thoroughly evaluate their electronic systems for potential security breaches. Staff education is also essential so that personnel understand how their actions might inadvertently provide access to a bad actor. Work with your administration and information systems personnel to assess your system and implement appropriate safeguards as well as develop a comprehensive staff education plan. Resources are available to policyholders in SVMIC's cybersecurity center found HERE on the Vantage® policyholder portal. SVMIC also recommends you talk with your professional business insurance broker to evaluate insurance coverage and determine a level of cyber coverage with which you feel comfortable in the event of a cyber incident.

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 or other HIPAA-related incident, contact SVMIC as soon as possible by calling 800-342-2239 and asking 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]https://www.nbcnews.com/business/business-news/cyberattack-cost-mgm-resorts-100-million-las-vegas-company-says-rcna119138

[2] https://www.forbes.com/sites/noahbarsky/2023/09/20/caesars-and-mgm-boards-lose-cybersecurity-gambles/?sh=279c17e64463

[3] https://www.aha.org/news/headline/2024-01-12-hospital-it-help-desks-targeted-sophisticated-social-engineering-schemes

[4] https://us.norton.com/blog/online-scams/what-is-phishing

[5] https://us.norton.com/blog/online-scams/vishing

[6] https://www.forbes.com/advisor/business/what-is-smishing/

[7] https://www.hhs.gov/about/news/2023/12/07/hhs-office-for-civil-rights-settles-first-ever-phishing-cyber-attack-investigation.html

Playing the Telephone Game: Can the Correct Diagnosis Win in the End?

By Kathleen W. Smith, JD

Do you remember playing the telephone game as a child? This is the game where the first player selects a word to whisper to the next player, and so on and so forth, until you see whether the final player ends up with the same word. The game challenges its players to listen carefully and make accurate identifications – did you hear the correct word to pass along, or did you misunderstand the word spoken to you and pass along an inaccurate word? In this closed claim, our "telephone game" began with our physician's accurate evaluation and diagnosis of his patient's condition. The "telephone game" was interrupted by one unsupported, unsubstantiated diagnosis appearing on a single medical record. The patient's lawyer seized upon that diagnosis, built a case around it, supported the theory with expert proof, and ultimately argued the theory to a jury. To win his case, our doctor was called upon to disprove the plaintiff's theory and convince the jury that his

explanation was accurate and true. Spoiler alert: he did just that!

Mr. Martin*, 95 years old, unfortunately fell at his home and broke his hip. After undergoing an uneventful surgical repair and subsequent hospitalization, Mr. Martin was transferred to the Subacute Care Unit of the hospital for rehabilitation and further care. Dr. Jones was his attending physician during his stay in the Subacute Care Unit. As is common with a patient his age, Mr. Martin had many pre-existing comorbidities, including an extensive history of bilateral lower extremity peripheral artery disease and peripheral vascular disease with prior right and left femoral bypass grafting. On Admission Day 1, Mr. Martin complained of left calf tenderness. Suspecting a blood clot, Dr. Jones ordered a venous Doppler ultrasound. This was negative for DVT. Some mild color changes were noted in his left foot over the next several days, but the tenderness resolved, and Mr. Martin was otherwise stable and progressing with his rehabilitation.

On Admission Day 8, however, Mr. Martin complained of significant pain in his left calf and marked color changes were noted in his left leg. Recognizing the sudden change in Mr. Martin's condition and cognizant of his medical history, Dr. Jones ordered a stat arterial Doppler ultrasound. This imaging revealed a complete occlusion in the patient's left femoral artery up to the popliteal bypass graft. After receiving this report, Dr. Jones emergently transferred Mr. Martin back to the hospital for further care from a vascular surgeon. The surgeon determined that Mr. Martin's left leg could not be salvaged, and a left above knee amputation was performed.

Oddly, and without any context or further explanation, the surgeon who performed the amputation documented in the Operative Report that the Pre- and Post-Procedure Diagnoses were "compartment syndrome left lower leg with ischemia noted x 2 weeks." Nothing in the medical record supported this diagnosis. In fact, the medical records from both the Subacute Care Unit and the initial admission directly contradicted compartment syndrome as an accurate diagnosis. Mr. Martin experienced a distinct change in his condition on the morning of Admission Day 8. Femoral artery occlusion was seen on stat ultrasound. The pathology from the amputation surgery confirmed an acute thrombosis with no evidence of widespread tissue necrosis. Instead of suggesting compartment syndrome as the cause, the clinical presentation, imaging, and pathology were instead consistent with the sudden development of a catastrophic occlusion that caused a rapid decline in the condition of the left leg.

In the lawsuit that followed, however, the plaintiff alleged that Dr. Jones failed to recognize, diagnose, and timely treat Mr. Martin's developing compartment syndrome, causing the need for amputation. The plaintiff's lawyer secured an expert who supported this theory. The plaintiff's expert testified at trial that a compartment syndrome was missed by Dr. Jones and was the cause of the amputation.

In defense of his care, Dr. Jones denied Mr. Martin ever actually had a compartment syndrome. Instead, Dr. Jones explained Mr. Martin's long history of peripheral vascular and artery disease. Mr. Martin experienced a sudden catastrophic event related to this pre-existing condition. Dr. Jones demonstrated how he promptly responded to this

emergency by ordering the appropriate diagnostic test and then transferring the patient emergently to the hospital for further care. Two defense expert witnesses who testified at trial were fully supportive of Dr. Jones' diagnosis and decision-making. Further, the defense experts also denied the existence of compartment syndrome.

During the trial, the jury was presented with two competing causation theories. Both theories were supported by physician expert witnesses. It was up to the jury to determine which theory to believe. At the end of the four-day trial, the jury agreed with Dr. Jones' explanation of what happened and returned a defense verdict in his favor.

To prevail in the telephone game, the players need to listen carefully. The same is expected of our treating physicians. Inattentiveness, even just one imprecise or assumed diagnosis in a medical record, can cause significant subsequent trouble. Here, it served as the foundation upon which the plaintiff built his lawsuit. However, Dr. Jones never doubted his opinion on causation, even in the face of the plaintiff's competing theory supported by an adverse physician expert. Always confident in his diagnosis, care, and treatment of Mr. Martin, Dr. Jones patiently waited for the litigation process to work its way through trial. And, like the winning team in the telephone game, Dr. Jones prevailed at trial with a jury who was equally patiently listening to the two competing theories of what happened, weighing them, and choosing the correct one.

*Names have been changed.

New! Medical Assistant Training Resource

By Stephen A. Dickens, JD, FACMPE

All aspects of human resources, especially the recruitment and orientation processes, consume a tremendous amount of time for the average practice. The Great Resignation forced medical groups to rethink their hiring and training processes in the current employee-driven market. One of the most difficult positions to fill is that of a medical assistant. While the struggle to find experienced employees continues, innovative practice executives are looking to non-traditional approaches and training their own medical assistants.

Medical assistants fill a pivotal role and often perform a wide variety of functions in a practice. Ensuring these individuals are well trained and qualified for the position is essential to efficiently assisting the practitioner, providing a positive patient experience, and managing the risks associated with a non-licensed individual involved in patient care. Since most states do not define the scope of practice for a medical assistant, it is essential that a practice carefully consider the MA's role since liability for their actions can be

imputed to the physician. While a formal and vetted training program is desirable, practices can build their own orientation programs with a thorough education and observation process. A skills checklist is a great way to begin assessing new and existing employee skills.

SVMIC is pleased to share with our members and their practice leaders our newly developed Medical Assistant Training Resource. The Medical Assistant Training Resource serves as a guide for practices to build their own training and orientation program. This resource is designed to be modified and customized to their specialty and practice model. Members and their staff may access the MA Resource on the Vantage® policyholder portal.

The MA Resource is one of the many ways SVMIC can help with your HR challenges. Our Medical Practice Services Consultants are available to assist with tough HR questions. Be sure to check out our HR Toolkit if you are not already using it.

Additionally, SVMIC can perform an assessment of your practice's culture to help you keep those great employees once you find them. A variety of educational topics are also available to supplement your professional development efforts with your team. Reach out to us at **ContactSVMIC@svmic.com** or 800.342.2239 and ask for Medical Practice Services.
