Risk Matters: Medical Malpractice Stress Syndrome

By Jeffrey A. Woods, JD

Medical malpractice lawsuits are extremely stressful, and a topic that is seldom discussed is Medical Malpractice Stress Syndrome ("MMSS"). MMSS involves having a traumatic reaction to a malpractice claim or lawsuit, impacting the provider's emotional and possibly physical health. The syndrome has been described as a "forme fruste" of posttraumatic stress disorder ("PTSD").[1] MMSS impacts not only the provider's well-being, personal and professional relationships, and ability to assist in their own defense, but can also affect patient safety during and after the litigation.[2]

One common recommendation to alleviate some of the effects of MMSS is provider empowerment via process knowledge and preparation.[3] Since knowledge is power, SVMIC's risk education programs for 2024 and 2025 will take a single medical malpractice lawsuit from pre-suit through the jury verdict. Click here for the 2024 live program schedule. Each phase of the litigation will be examined through the eyes of an experienced defense attorney, and recommendations will be given as to how providers

can better assist in their own defense.

Providers who believe they have or may have MMSS should discuss with their defense attorney and their SVMIC Claims attorney. Additionally, there are resources available in the Litigation Support section on the Vantage® policyholder portal. However you go about it, providers should seek appropriate professional help as necessary. MMSS is far more common than most providers would believe and asking for help is not a sign of weakness.

[1] Paterick ZR, Patel N, Chandrasekaran K, Tajik J, Paterick TE. **J Med Pract Manage**. 2017; 32:283–287.

[2] Vizcaíno-Rakosnik M, Martin-Fumadó C, Arimany-Manso J, Gómez-Durán EL. **J Patient Saf**. 2022; 18: 46–51.

[3] Charles SC. Coping with a medical malpractice suit.**West J Med**. 2001; 174:55–58.

Closed Claim: Communication Breakdown

By Jeff Williams, JD

"Communication breakdown, it's always the same
Havin' a nervous breakdown, drive me insane" – Lyrics from "Communication Breakdown" by Led Zeppelin

The truism here is communication breakdowns, in a healthcare setting, will drive us all insane. But there are many ways breakdowns happen, and it's usually not the same.

Communication between the many medical professionals who are caring for a patient with a critical condition can be a life-or-death matter. Hospitals and physicians' offices have systems in place so that communication across all providers is executed effectively. Protocols, electronic medical records, cell phones, call services, secure messaging systems, and, in this story, pagers (aka "beepers")[1] are used to establish lines of communications amongst the many healthcare providers involved in the care of each patient. Even when multiple systems function properly, providers must proactively

participate in the process for patient care to be carried out in a safe manner. The consequences in a healthcare setting can be dire when there are multiple breakdowns in communication.

Mary Cutler[2] was a 71-year-old retiree who presented on a Friday to the emergency department with complaints of significant chest pain for three days. Cardiologist Dr. Mays Cario took over her care from the E.D. and admitted Mrs. Cutler onto the telemetry floor. Prior bloodwork obtained at an outside rural hospital revealed elevated troponin indicative of an NSTEMI (Non-ST-Elevation Myocardial Infarction). She was started on a heparin drip and a statin. An echocardiogram showed reduced cardiac function. Mrs. Cutler was told that a diagnostic catheterization was necessary. She had expressed a general distrust of doctors and told Dr. Cario not to perform any unnecessary procedures that would "run up the bills." Her initial hesitancy in deciding to undergo the diagnostic procedure caused a delay into the weekend. Ultimately, she consented to the diagnostic catheterization which occurred on Saturday. While the results indicated a severe coronary blockage, Dr. Cario deemed her condition non-emergent as her chest pain had subsided. After being told the results of the diagnostic procedure, Mrs. Cutler agreed to a stenting procedure. Because it was the weekend, she was scheduled for a percutaneous coronary intervention the following Monday.

Hospitalist Dr. Seth Patel was working at the hospital over the weekend. The hospital nursing staff was tasked with monitoring Mrs. Cutler until the stenting procedure could be performed. On Sunday evening, she complained of back pain which was relayed to Dr. Patel. He ordered an EKG, CT scan, and lab work. The EKG indicated concerning changes in Mrs. Cutler's cardiac condition showing ST segment elevations, but the results were not regarded as requiring urgent attention. Less than two hours later, a nurse informed Dr. Patel by phone that Mrs. Cutler's blood pressure was low, and she was again complaining of chest pain. Mrs. Cutler was repositioned, and a saline bolus was ordered. She was put on a vasoconstrictor to increase her blood pressure. During this time, Dr. Patel ordered her to be moved to the ICU. Another EKG was obtained, again indicating concerning results, but not recognized as critical. In hindsight, had the second set of EKG results been recognized as urgent, the hospital's STEMI protocol likely would have been invoked, necessitating immediate cardiac intervention.

While being transferred to the ICU, Mrs. Cutler asked a nurse, "Am I going to die?" She knew something was gravely wrong and was noted to be blue in the face. In an apparent attempt to convey the urgency of the patient's condition, a nurse sent a report to Dr. Patel indicating that the patient had asked if she was going to die. Mrs. Cutler also asked to be seen by a physician. Dr. Patel was the physician in the hospital responsible for her care. He never saw her in person; opting to communicate with the nursing staff by phone.

Once Mrs. Cutler was in the ICU, a nurse attempted to contact the cardiologist, Dr. Cario, by various means. There was an appreciable delay in getting in touch with him. Later, a nurse was finally able to reach Dr. Cario on his cell phone. He was on his way into the hospital. Mrs. Cutler went into cardiac arrest while undergoing the CT scan. Unfortunately,

resuscitative measures administered by the nursing staff were unsuccessful. By the time Dr. Cario arrived at the hospital, it was too late.

Throughout these events, Dr. Cario and Dr. Patel never communicated in any manner.

The family filed a lawsuit naming Dr. Cario, Dr. Patel, and the hospital as defendants, alleging various acts of negligence that led to the untimely death of Mrs. Cutler. The case was focused on the lack of communication between the hospital nurses and the physicians involved in the care of Mrs. Cutler. Throughout the case multiple depositions were taken of family members, hospital nurses, and the physicians. The testimony showed that each side had its own take on who was communicating and who was not. As usual, each party produced multiple medical experts to bolster their positions. The Plaintiff would eventually pursue distinct theories against the hospital, Dr. Cario, and Dr. Patel. The cases against the two physicians are detailed below.

Attempts to Contact the Cardiologist

Dr. Cario maintained throughout the suit that he should have been contacted sooner than he was. Not surprisingly, this was one of Plaintiff's theories of the case also. He testified in his deposition that he should have been called when the first EKG reflected signs of cardiac distress. Mrs. Cutler was also experiencing chest pain, low blood pressure and other symptoms on Sunday evening, yet another reason to call the cardiologist.

When the hospital staff tried to contact him, he could not be reached. The multiple attempts to contact Dr. Cario were as follows: 1) by pager; 2) by a secure messaging system maintained by the hospital; 3) by a call service at his office; and 4) by his cell phone. The first three methods of communication did not result in a response from Dr. Cario. Ultimately, a nurse was able to contact Dr. Cario by calling his cell phone number.

There were several issues with the attempts to contact Dr. Cario. First, Dr. Cario no longer used his pager. In fact, he believed the number was disconnected. Nonetheless, the pager number was listed in the hospital system as a preferred way to contact Dr. Cario. Next, when the nurse called Dr. Cario's answering service on Sunday night, the service responded that it did not know how to contact Dr. Cario and suggested that the nurse call Dr. Cario's office (on the weekend). When the nurse sent a message through the secure messaging system, Dr. Cario was unaware that he had received the message.

The Case Against the Hospitalist

A concerning allegation against Dr. Patel was that he never saw the patient at bedside, even though he was at the hospital the entire weekend. This was despite Mrs. Cutler's deteriorating condition, and her request to be seen. While not physically seeing the patient was defensible from a standard of care perspective, it was anticipated that Plaintiff's counsel would bring this to the jury's attention at trial. The optics were concerning. In addition to not seeing the patient, the EKG results that went unrecognized as critical were problematic for the defense. The proof developed through Plaintiff's medical experts

suggested that if Dr. Patel or a nurse had contacted Dr. Cario earlier, the outcome would have been different. Plaintiff's expert hospitalist laid out a timeline in his deposition which strongly implied that if Dr. Patel had intervened earlier, Mrs. Cutler would have had a greater chance of surviving. As expected, Plaintiff's experts were highly critical of Dr. Patel for not seeing the patient at bedside and never communicating with Dr. Cario.

While each defendant was able to disclose medical experts supportive of their positions, the case had weak points that Plaintiff's counsel could exploit at trial. The reality was Mrs. Cutler suffered from a condition that was treatable if medical intervention had occurred earlier. Further, it became clear there was going to be finger pointing between the hospital, Dr. Patel, and Dr. Cario related to the various communication issues. Most cases only get better for the plaintiff when defendants blame each other. The decision was eventually made to settle and avoid the substantial risk of an adverse verdict if the case was tried.

The Takeaways

- In cases where communication among providers is in question, call logs, digital messages (text messages, secure messages, text messages, and emails) are all trackable. The physician should expect that the messages will be requested and scrutinized in the discovery phase of litigation. *Whether or not the messages are responded to will be evident.* Keep in mind, while the content of the message was not in question in this case, be cautious not to make comments that will be used against you in the future. Communicate as if each message will be scrutinized. Keep it professional.
- For providers working in hospitals, an office setting, or other medical facilities that will need to contact you on an emergent basis, be sure your up-to-date contact information is on file at the facility. Check it periodically.
- While medical care can be communicated over the phone or by various messaging services, if it is possible to physically see a patient that has a critically acute condition, consider doing so.
- Be proactive, not passive in your communications. Practitioners should not hesitate to pick up the phone and call the specialist involved in the patient's care.

[1] According to Wikipedia, pager usage in America was in rapid decline by 2002. See https://en.wikipedia.org/wiki/Pager.

[2] Names have been altered.

Physician Payment Issues in the Wake of the Change Healthcare Hacking

By Elizabeth Woodcock, MBA, FACMPE, CPC

The results of an American Medical Association survey in the aftermath of the February 21 Change Healthcare cybersecurity attack demonstrate the continuation of challenges, despite parent company United Healthcare's declaration that the situation has been resolved. The April 29, 2024 AMA survey reveals:

- 60% of medical practices continue to face challenges in verifying patient eligibility.
- 75% still face barriers with claim submission.
- 79% still cannot receive electronic remittance advice.
- 85% continue to experience disruptions in claim payments.

More distressing, these challenges are resulting in cash flow issues that are forcing physicians to seek loans or go without personal compensation to avoid disrupting patient care. While there are no easy solutions, medical practices can take steps to navigate these uncharted waters.

Recognize key government interventions. The US Department of Health & Human Services has issued requirements for its Medicare contractors. For example, "the MACs [Medicare Administrative Contractors] must accept paper submissions if a provider needs to file claims in that method." The department, which includes the Centers for Medicare & Medicaid Services (CMS), has issued instructions to the states about Medicaid payments. Of particular importance is the resource guide the federal agency compiled and distributed to providers in March.

Identify payment relief opportunities - and the strings attached. Proactively seek financial resources available, including the Change/Optum program. Some accountable care organizations have stepped up to the plate to offer advance payments. Read the fine print before applying, however, as programs may have arduous application processes and challenging mechanisms for payback. Although far from ideal, some practices have found a business line of credit or loan from a bank the most effective option.

Track the progress. The February 21st cyberattack that hit Change Healthcare was initially thought to just affect claims distribution. However, the situation has affected many aspects of the health care data highway, including prescriptions and prior authorizations. Monitor the progress by function.

Measure the impact. While the media is full of anecdotes, let's identify the impact of the cyberattack on your practice. Tracking claims has always been important. Today, it's critical. Develop a report to pinpoint the claims that were not released and/or processed, documenting the date and associated charges. Maintain a record of your attempts to submit the claims, even if they do not get processed. That record will help you if you get denied for timely filing, an aftermath of the incident that practices around the nation are reporting. Appeal timely filing denials until you're successful in getting paid, reporting to your state insurance commissioner if you are not. Maintain meticulous records regarding the unprocessed claims, as well as those that have been denied. Consider reporting your efforts and (blinded) data to advocacy groups who are working with state and federal legislators to compensate providers for their financial losses.

The past decade has seen consolidation of the major insurance companies -- United Healthcare, which bought Change Healthcare in October 2022 - is a nearly $400-billion company. Not only does it control approximately 40% of health care claims processed each year in the United States, United Healthcare now employs 1 out of every 10 physicians. The cyberattack has put the company in the spotlight of federal lawmakers. Called to testify before Congress on May 1, CEO Andrew Witty's attestation underscores how much remains unknown about the attack itself - and the implications for the future. United Healthcare admitted that elementary safeguards were not present - hackers gained entry via a portal that did not have basic multi-factor authentication in place. Despite the $22 million ransom payment by United Healthcare, the Russian hackers

have begun posting sensitive medical records on the dark web, including charts from U.S. military personnel. United Healthcare's documented vulnerability - and their massive size -- may not bring comfort to physicians. The only promising news that may have come out of this nightmare is that United Healthcare is squarely on the radar screen of lawmakers. Whether physicians may benefit from this scrutiny will likely take years to understand.

Managing Vendor Risk: Lessons Learned After the Change Healthcare Breach

By Brian Johnson

The healthcare sector was dealt another blow on February 21, 2024, when Change Healthcare, a division of Optum and a subsidiary of UnitedHealth Group Incorporated, fell victim to a cyberattack. The company disclosed that the attack compromised customer data and disrupted operations, leading to a shutdown of customer-facing services. This interruption had a significant ripple effect, affecting an estimated one-third of all medical transactions in the U.S.[1], highlighting the critical role Change Healthcare plays in the nation's healthcare infrastructure.

Many medical practices were unable to process claims, verify insurance eligibility, access patient records, and conduct routine billing. As a result, the disruption caused lost income and forced some offices to temporarily close. This incident raises many questions

regarding Change Healthcare's security practices and how an organization can protect itself from the same fate. This article highlights a crucial lesson about the risks of vendor dependency in the healthcare sector.

What Happened

Change Healthcare fell victim to a Russian-linked hacking group named BlackCat known for its expertise in ransomware attacks. The group exploited a vulnerability in a product called ConnectWise to infiltrate Change Healthcare's systems. Upon gaining access, they exfiltrated 6 terabytes of data containing protected health information (PHI) then launched a ransomware attack locking the company out of their systems[2].

Immediately following the detection of the incident, Change Healthcare initiated a shutdown of systems and services to contain the attack and prevent further spreading of the ransomware. The result of the massive shutdown left healthcare organizations helpless as they lost access to Change Healthcare services upon which they depended. Furthermore, these organizations were left in the dark for nearly a month before the first systems were restored.

Financial Impact on Health Organizations

The Change Healthcare incident significantly impacted a range of clearinghouse operations that included medical records, insurance, billing, and prescriptions. The resulting absence of these services placed financial strain on many health organizations. According to the American Hospital Association (AHA) 94% of hospitals reported a financial impact[3], and an American Medical Association (AMA) survey of medical practices reported that 77% of respondents experienced service disruptions, with 80% reporting lost revenue from unpaid claims, and 55% having to use personal funds to cover their practices' expenses[4].

In response, Optum has established a Temporary Funding Assistance Program to assist medical practices that are unable to meet their weekly shortfall[5]. Additionally, these events prompted the Centers for Medicare and Medicaid Services (CMS) to issue accelerated and advanced payments to affected providers[6]. These measures aim to provide financial relief to healthcare providers impacted by recent challenges.

Scrutiny of the Change Healthcare incident continues as this event has prompted numerous investigations, class action lawsuits, and calls to Congress. On March 13, the Department of Health and Human Services (DHHS) issued a letter stating that the Office for Civil Rights (OCR) would be opening an investigation focusing on whether a breach of protected health information occurred and compliance with the HIPAA Rules[7].

Making Vendor Management Part of Risk Management

Medical practices depend on third-party vendors for essential services critical to their daily operations, and they depend on these services being consistently available while protecting the confidential information entrusted to them. However, the Change Healthcare breach, along with its subsequent cascading effects, highlights the risks associated with reliance on vendors, particularly when a single vendor provides multiple services. Consequently, healthcare organizations must be prepared for potential disruptions and should incorporate specific strategies into their business continuity and disaster recovery plans to mitigate these risks.

Conduct a Risk Assessment

A risk assessment focusing on vendor management is an essential first step in preparing for future disruptions. Organizations should conduct a review of essential services provided by third-party vendors, identifying those that are critical for day-to-day operations. This process involves not only recognizing which services are vital but also understanding the potential consequences of their failure. By mapping out how each service contributes to the organization's overall functionality and identifying potential work arounds, practices can ensure ongoing operations during unexpected vendor outages.

For each identified service, organizations should establish potential contingency solutions. These solutions could range from manual processing to alternative communication channels and the use of redundant vendors. For instance, if the current electronic process fails, is it feasible to revert to manual, paper-based operations? If so, organizations must ensure they have the paper documents and other resources necessary to carry out these tasks effectively.

During incidents like the Change Healthcare breach, where online electronic portals became inaccessible, organizations found themselves at a loss. To prepare for similar future scenarios, it's vital to consider how alternative processing might be executed. Options could include emailing or faxing documents directly to the vendors. Of course, the privacy and security of protected health information must be maintained when alternate processing methods are in use.

It's essential for organizations to identify and vet alternative vendors well in advance. This preparation involves understanding the specific requirements needed to establish service quickly and efficiently. Establishing these relationships and processes ahead of time ensures that, in the event of a disruption, organizations can migrate without significant delays. Service agreement terms with alternate vendors should be reviewed for understanding any contractual limitations or conditions for quickly bringing the secondary provider on-line. In addition, businesses should not wait until a crisis occurs to start identifying potential vendors. Proactive relationship management, with a clear plan for

transitioning services during an incident, is crucial.

Plan for Revenue Disruptions

During the Change Healthcare outage, many medical practices continued services while revenue streams were disrupted. As part of the risk assessment, organizations need to identify potential impact on revenue and its impact on continued operations. Monthly expenses for payroll, utilities, rent, and other core functions should be determined, along with evaluating how long the organization can sustain these expenses without normal revenue inflow. This analysis will enable practices to identify the necessary buffer to support operations during extended periods of disruption.

Alternative solutions to consider include insurance, cash reserves, and lines of credit. Business Interruption Insurance is designed to compensate businesses for lost income due to external factors beyond their control, but like any other insurance, it is important to understand what is and what is not covered, as well as reporting obligations and policy limits. Cash reserves provide a financial cushion that can help a business stay afloat without the need for reliance on external funding during short-term disruptions. Similarly, lines of credit offer flexible, readily available funds that can be used to manage unexpected expenses or cash flow shortages. It's crucial that these measures are established well before any incident occurs.

Conclusion

The Change Healthcare breach serves as a stark reminder of operational risk imposed by third-party vendors, particularly the reliance of a single vendor for multiple core services. To combat such vulnerabilities, it is necessary for organizations to include vendor management in the broader risk management framework. This should include conducting thorough risk assessments focused on the operational dependencies on third-party services. Furthermore, the financial impact of the Change Healthcare breach underscores the necessity of planning for revenue disruptions. In conclusion, the lessons learned from the Change Healthcare incident are clear: healthcare organizations must not only prepare for the possibility of their own technological failures but also plan for disruptions caused by third-party vendors.

Resources are available to policyholders in SVMIC's cybersecurity center found HERE on the Vantage® site. 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 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.

Supporting Hospitals and Patients After Cyberattack on Change Healthcare (AHA.org)

UnitedHealth Confirms Data Theft From Change Healthcare (crn.com)

Information on the Change Healthcare Cyber Response (UnitedHealthGroup.com)

AHA Survey: Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals' Finances (AHA.org)

Temporary Funding Assistance Program for Providers (optum.com)

Change Healthcare/Optum Payment Disruption (CHOPD) Accelerated Payments to Part A Providers and Advance Payments to Part B Suppliers (CMS.gov)

Cyber Attack on Change Healthcare (hhs.gov)
