THE MONTHLY PUBLICATION FOR CAP MEMBERS

CAPsules®

COOPERATIVE OF AMERICAN PHYSICIANS

Risk Management and Patient Safety News

You Deserve to Be Safe at Work

by Deborah Kichler, RN, MSHCA

September 2019

Pop! Pop! Pop! Imagine hearing this unexpected sound in an office building, and then you see a person waving a firearm with active rounds.

Workplace violence is on the rise and in healthcare there is no exception. The first line of defense is preparation. Directives on the response to workplace violence should be developed and integrated fully with all other simulated disaster drills, such as those developed for earthquakes or power outages. Hospitals and some offices include regular education and drills on what to do in the event of violence in the workplace, including active shooter scenarios.

Physician safety, and that of his or her staff, is an issue all need to consider. Offices see patients with mental health imbalances, patients in need of pain management, patients and staff struggling with personal issues, and patients with addictions. Unfortunately, healthcare professionals sometimes become the target of their patients' anger and often unforeseen recipients of their violent outbreaks. What can you do?

Practical measures for the office:

- Be alert as you enter and leave the building.
- Set up exam rooms so the patient is not between you and the door.
- Train staff to de-escalate and defuse tense situations (have protocols in place, practice drills as a team).
- Review OSHA and CDC resources for minimizing workplace violence and managing conflict.
- Involve local law enforcement in your training and drills.
- Review CAP's Risk Management Institute Program (Effective Office Communication, Patient Education).

The Occupational Safety and Health Administration (OSHA) defines workplace violence as any physical assault, threatening behavior, or verbal abuse occurring in the workplace setting. While federal law does not impose a duty on employers to prevent workplace violence against employees, OSHA mandates that employers provide a safe working environment and requires employers to provide a workplace free from recognized hazards that are causing, or are likely to cause, death or serious physical harm to employees. It is important that employers take an active approach to control these risks and associated exposures.

There are four key categories of workplace violence: Personal Relationships, Employee-on-Employee, Customer/Client, and Criminal Intent. Common triggers for workplace violence include: domestic violence/marital or relationship problems, job-related stress or frustration, workforce reduction, alcohol/drug abuse, romantic interest in a coworker, and disgruntled patients and visitors. How you respond to specific situations is critical.

Perform an office risk analysis. Identify strengths and weaknesses of your office violence prevention plan. Integrating safety in a culture of respect and trust creates a positive work environment. Require all staff to undergo training in responding to a patient's family members who are agitated and potentially violent. Training should focus on prevention, verbal de-escalation skills, and personal safety. Effective training involves role playing, simulations and drills because if you don't rehearse, it won't work in a real-life situation. It is also essential to include education on procedures for notifying supervisors and security staff. Encourage employees and other staff to report

continued on page 2

Continued from page 1

incidents of violent activity and any perceived threats of violence. Have processes in place for post-incident debriefing and follow up. Have your plan in writing and have it accessible to employees at all times.

When dealing with disruptive behavior, verbal threats, use of profanity, acts of physical threat, and refusal to comply with reasonable requests from an office team member, place the person somewhere away from onlookers with as little environmental stimulation as possible. Listen and acknowledge the person's concerns. De-escalate the situation as much as possible. Call for assistance.

Everyone in the office has a responsibility to contribute to preventing, identifying, responding to, and recovering from incidents of workplace violence. Important questions to consider are:

1. Do you have a team or personnel to develop, review, and implement policies to deal with violence?
2. What is the office plan for maintaining security?
3. What is the strategy for maintaining a safe and secure environment?
4. Know how to contact law enforcement authorities.
5. What do you do in an active shooter scenario? A consultant on safety issues with the FBI gives the following advice:

   RUN - Know which exits to use. Leave your belongings behind. Evacuate regardless of whether others agree to follow. Keep your hands visible.

   HIDE - Know where to hide. Hide in an area out of the shooter's view. Lock or block entry to your hiding place. Remain quiet.

   FIGHT - Know what office equipment to use as a weapon. Fight as a last resort and only when your life is in imminent danger. Improvise weapons or throw items at the active shooter. Commit to your actions … your life depends on it.
6. Provide event debriefing and availability of trauma counseling for all employees.
7. Conduct a risk analysis of your practice's emergency plan to identify opportunities for improvement.

The office practice team responsible for the workplace violence management program may also be responsible for developing an active shooter response plan in collaboration with local law enforcement and emergency management responders. The International Association for Healthcare Security & Safety (IAHSS) has developed general guidelines for management of an active shooter in a healthcare facility that reference the "Active Shooter Handbook — How to Respond" and the Department of Homeland Security.

We live in a time of high anxiety, stress, and misinterpreted communications. Taking the time to communicate clearly with each other, be it coworker, patient, or family member, can hopefully alleviate the stress and fears of underlying health issues. Working together and being prepared are pivotal to a safer response in the event of emergent situations. We all deserve to work in a safe environment.

Deborah Kichler is a Senior Risk Management Specialist for CAP. Questions or comments related to this article should be directed to dkichler@CAPphysicians.com.

Resources:

"Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide." November 2015

OSHA Workplace Violence • www.osha.gov

"Workplace Violence Prevention Strategies and Research Needs." Department of Health and Human Services

"Preventing HealthCare Workplace Violence Toolkit." April 2017 Washington State Hospital Association

"Physician Office Risk Management Playbook." American Society for Healthcare Risk Management

e-Evolve: Active Shooter Response • CAPAdvantage • http://www.capphysicians.com/practice-management-services#capadvantage

Federal Bureau of Investigation • https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-resources

CAP website resources: Safety and Security

http://www.capphysicians.com/practice-management/practice-management-services/cap-marketplace

ACT Attack Countermeasures Training

Alon Stivi (Irvine) • 949-355-4885 • https://www.actcert.com/

Embassy Consulting Services, LLC

Josef Levy, President (Southern California) • 562-577-5874
embassycs@ymail.com • https://embassyconsultingservices.com/

Discount: 20% for CAP members

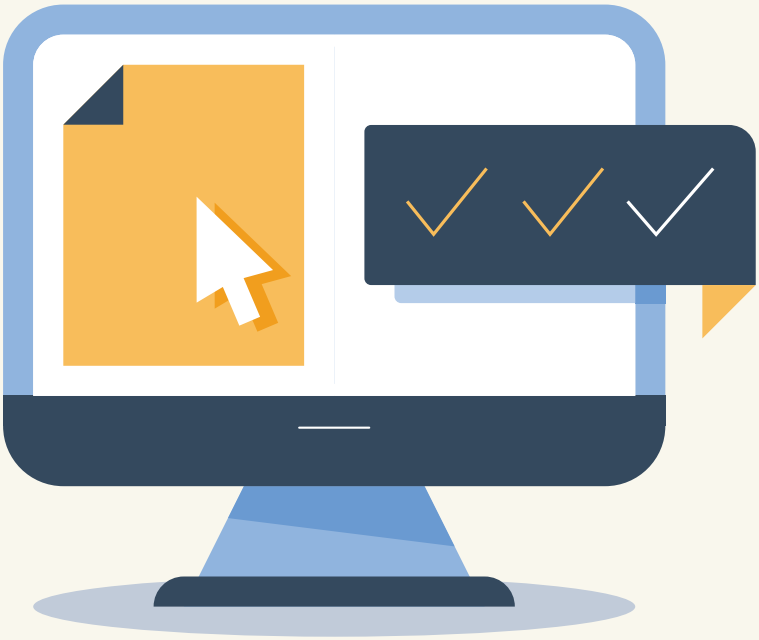
Embassy specializes in designing and delivering quality training programs, including Workplace Violence & Active Shooter Training. They also conduct security site assessments.

The Urban Survival Chick - Prepare, Prevent and Protect

Maryanne Morcos (Los Angeles)
mary@urbansurvivalchick.com • http://urbansurvivalchick.com

Tips to Prepare for 2020 Open Enrollment

CAP Members Can Take Advantage of Top-Rated Personal Insurance Programs



September 2019

Did you know that your CAP membership includes access to a dedicated insurance agency? This means that you not only receive as part of membership — at no additional cost — life, group disability, and cyberrisk protection (among other valued-added coverages), but also access to purchase superior business and personal insurance all through one convenient source at favorable rates.

During the 2020 open enrollment period, CAP members will have the opportunity to add additional coverage to their existing policies or sign up for new coverage. In addition to supplemental short- and long-term disability, the following programs will also be available during the open enrollment period:

- Enhanced dental and vision insurance for individual physicians and their families
- Critical illness insurance
- Accident insurance
- Life insurance

Here Are Things You Can Do Now to Prepare

1. Review your current policies and coverage.
2. Assess your current personal and business needs and any major changes within the past year.
3. Begin collecting required information: Social security numbers, beneficiary information, etc.
4. Review available coverage programs at www.capphysicians.com/business-and-personal-insurance.

Our goal is to ensure that all CAP members have a comprehensive overview of their available benefits so you can make informed decisions on what kinds of coverage are best for you, your family, and your practice for the coming year.

More information about the open enrollment period will be available in October. Don't miss important emails from CAP that will include details on rates and how to enroll. Contact us today at 800-819-0061, or at CAPAgency@CAPphysicians.com.

CAP PHYSICIANS INSURANCE®
License No. 0F97719

A Good Outlook for Payments of E/M Visits

by Gabriela Villanueva

Public Policy

In the fall of 2018, the Centers for Medicare and Medicaid Services (CMS) released the proposed 2019 Medicare Physician Fee Schedule (MPFS) rule addressing Medicare payment rates and policy provisions for physicians in 2019. While the rule included welcomed proposed reductions in medical history and exam documentation requirements, the portion that suggested the collapsing of levels 1-5 payments on the MPFS for evaluation and management (E/M) visits into single payments by blending levels 2-4 into one payment rate starting in 2021 received immediate pushback and criticism from the physician community, forcing CMS to delay its implementation.

On July 29, 2019, the CMS released yet another set of rules for calendar year (CY) 2020, but there are no significant updates for E/M coding, payment, or documentation requirements for CY 2020, as it was established in the 2019 rule that changes would not issue until CY 2021.

In the latest released set of a 1,200+ page rule on July 29, CMS included proposed changes, as suggested by the American Medical Association (AMA), to payments for E/M visits starting in CY 2021. Below is a basic summary.

Proposed payment changes for E/M visits in CY 2021:

1. Maintain a separate payment rate for all E/M levels, although it is being proposed to delete CPT code 99201 (Level 1 new patient office/outpatient E/M visits).

2. In addition to the base E/M visit levels, create two ADD-ON codes/descriptors that could be reported with an E/M visit:

a. Code 99XXX to describe a prolonged office/outpatient visit when time is used for code level selection and the time for a Level 5 office/outpatient visit is exceeded by 15 minutes or more on the date of service.

b. Code GPC1X would describe the work associated with visits that are part of ongoing, comprehensive primary care and/or visits that are part of ongoing care related to a patient's single, serious, or complex chronic condition.

While things will remain the same in CY 2020, it should be noted that the changes proposed for CY 2021 in this area are the result of the healthcare community making its concerns known and then working with the agency to find better solutions. As a result, the proposed rules overall appear to provide the increased flexibility for a physician to best and more accurately reflect his or her care of a patient, meet patients' needs with less burden, and receive proper compensation.

The January 1, 2021 implementation will allow time for provider education, updates to EHRs, and changes to workflow.

Gabriela Villanueva is CAP's Public Affairs Analyst. Questions or comments related to this article should be directed to gvillanueva@CAPphysicians.com.

Case of the Month

by Gordon Ownby

Even with the Best Preparation, Errors Will Happen

When this column addresses adverse events, we frequently try to identify some action or inaction that if addressed differently, might have led to a better outcome. Though thankfully rare, errors nevertheless can occur even with a spotless work-up.

A 53-year-old patient first visited Dr. GS, a general surgeon, complaining of a lump in her right breast. An ultrasound from two months earlier showed a lesion at 10 o'clock, and upon examination, Dr. GS noted a small but definite non-mobile mass. Dr. GS recommended an excision and several months later, he performed a right breast lumpectomy.

Pathology results for the excision showed a 1.4 cm invasive, moderately differentiated, ductal carcinoma, stage 1A. Dr. GS discussed the results with his patient and documented an early plan for a probable mastectomy and axillary node biopsy, pending the final pathology report and an oncology consult.

When the final pathology report was available later that month, Dr. GS discussed with his patient (with her two daughters interpreting) his assessment of invasive right breast cancer and the options for mastectomy versus conservation. Dr. GS charted the patient would "like to hear more about reconstruction as is leaning towards mastectomy." In order to assess her options, the patient was to undergo a bilateral breast MRI and have oncology, radiation oncology, and plastic surgery consultations.

While pursuing those consultations, the patient and Dr. GS discussed lumpectomy versus mastectomy over the next several visits, with the patient "still leaning towards conservation." Dr. GS explained that even with a partial mastectomy, the nipple needed to be removed. Dr. GS documented that his patient had been told by her plastic surgeon that reconstruction after a partial mastectomy with nipple and areolar excision was not possible. The patient nevertheless stated her preference for a lumpectomy and conservation. She signed a consent for a wide local excision, including the areola and nipple.

On surgery day, the patient was admitted for a "right partial mastectomy," which was noted as the chief complaint on the hospital admission sheet. However, Dr. GS performed (and described in his final report) a right breast mastectomy and lymph node biopsies. Though the pathology report described the procedure to be done as a "right partial mastectomy and removal of areolar/nipple complex" the report described the specimen submitted as "right breast mastectomy." The lymph nodes were negative for malignancy.

In a follow-up office visit two days later accompanied by a daughter, the patient complained of pain and asked Dr. GS why he performed a mastectomy. Later that day, Dr. GS reviewed the records and noted the patient's consent for a partial mastectomy. He called the patient and, through her daughter, acknowledged the error and offered his sincere apologies. Further follow-up office visits by the patient were uneventful. A lawsuit by the patient closed without going to trial.

Remarkable in the review of the medical records (including the customary "time out" in the operating

continued on page 6

Continued from page 5

room) was the absence of any factor to explain Dr. GS's performance of a different procedure than planned. (Though one of his early notations, that the patient would "like to hear more about reconstruction as is leaning towards mastectomy" is a bit incongruous, Dr. GS's subsequent charting is clear that the patient was leaning toward, and ultimately consented to, a partial procedure.)

This column typically strives to find a teachable moment in a bad outcome, usually by identifying some risk management shortfall in a fact pattern. Sometimes, of course, we humans can make mistakes even while taking all customary precautions. There's a lesson in that as well.

Gordon Ownby is CAP's General Counsel. Questions or comments related to "Case of the Month" should be directed to gownby@CAPphysicians.com.

Update Your Membership Information to Help with Your Year-End Planning

If you are contemplating a change in your practice, please notify CAP as soon as possible so our Membership Services Department can review your options with you and make your coverage transition a smooth one. Changes include, but are not limited to:

- Retirement from practice at age 55+
- Part-time practice
- Reduction or change in the scope of your practice
- Employment with a government agency or non-private practice setting
- Employment with an HMO or other self-insured organization
- Joining a practice insured by another carrier
- Moving out of state
- Termination of membership

The Board of Trustees of the Mutual Protection Trust will levy an assessment in November 2019. To allow ample processing time, we recommend that members advise us in writing no later than October 31, 2019, of any of the above changes to be considered eligible for waiver or proration of the next assessment.

To make an update, please log in to the Member's Area of the CAP website. Upon logging in, you will be prompted to **Update/Verify Your Information Now**. Our online Membership Information Update Form takes less than five minutes to complete.

If you have not yet registered for the Member's Area, please register for an account at https://member.CAPphysicians.com/register. You will need your member number and last four digits of your Social Security Number.

How One Wrong Click Cost a Practice $1M

Recently, one of CAP's member practices experienced a ransomware incident involving multiple office locations and servers, as well as thousands of patient medical records. Ransomware is a type of malicious malware designed to deny access to your computer system or data until a ransom is paid. It is one of the most common types of data breaches to affect medical groups.

When one of the practice's employees inadvertently clicked on a "phishing" email, malicious malware infected the main server and four virtual servers, locking the electronic health records and billing data for all three of the practice's locations.

Soon after, the practice received a ransom notice demanding $250,000 in Bitcoin, the equivalent of $1.5M, in order to release the encrypted files.

After several unsuccessful attempts to negotiate the ransom, the practice was unable to access its patient files.

Recovering the files proved to be an expensive and arduous task. Most firms quoted a cost upward of $250,000 with only a 50 percent success rate of full file recovery. Eventually, the practice's own IT firm was able to recover files dating to April of 2017.

The practice estimates that the loss of revenue to date is at least $1M.

What All Medical Practices Should Know About Ransomware

Ransomware typically spreads through phishing emails or by an employee unknowingly visiting an infected website. The ransom payment is usually in the form of Bitcoin and, even if paid, there is no guarantee you will get your data back.

Phishing is when a fraudulent attempt is made, usually through email communication, to steal personal information such as passwords, credit cards or account numbers. These emails often look like they are from a legitimate company or even someone you may know in order to trick you into sharing personal information such as credit cards or passwords.

How Can You Prevent Your Practice from Falling Victim to Ransomware?

- Educate your employees on ways to recognize a fake email:
  - Unfamiliar Tone or Greeting — legitimate emails usually call you by name
  - Sensitive information is requested such as passwords
  - Domain name is misspelled or does not match the company who sent it
  - The email forces you to click a link to go to a website or it contains suspicious attachments
  - The email is poorly written
  - The email message displays a sense of urgency to act
- Make sure your servers are securely backed up in real time so if you need to recover data, it will be up to date.

Even when you implement these precautionary measures, it is still possible to be impacted by a ransomware data breach. CAP provides all of our members with a $50,000 CyberRisk policy, but as you can see, this may not be enough. Make sure you have adequate data breach insurance to protect you. The cost of protection could be a fraction of the cost of a ransomware attack to your business.

Contact CAP Physicians Insurance Agency to get a quote for additional coverage up to $1,000,000 via email CAPAgency@CAPphysicians.com or call 800-819-0061.

COOPERATIVE OF
AMERICAN PHYSICIANS

Cooperative of American Physicians, Inc.
333 S. Hope St., 8th Floor
Los Angeles, CA 90071

September 2019

IN THIS ISSUE

CAPsules® is a publication of the Corporate Communications Department of the Cooperative of American Physicians, Inc.
333 S. Hope St., 8th Floor, Los Angeles, CA 90071 | 800-252-7706 | www.CAPphysicians.com.

We welcome your comments! Please submit to communications@CAPphysicians.com.