



Celebrating Our CAP Community Heroes

A Call for Nominations!

Above and beyond. It's a phrase that may be a bit worn around the edges, but in the hands of a compassionate and motivated healthcare professional, it can be an incredibly powerful force for good.

That's the idea behind CAPtivating Causes, CAP's community service program, and our annual **Community Hero** and **Community Leadership Awards**. Since 2019, these awards have celebrated the extraordinary efforts of CAP members who provide critical medical care to patients in need and also go above and beyond the call of duty to make a difference in their communities.

CAP values the active engagement of our physician members in their communities, throughout the state of California. Our CAPtivating Causes program is a way to shine a spotlight on their charitable service and encourage other physician members to join in the effort.

For 2022, we're particularly interested in hearing the stories of members have been volunteering their time and talents through a charitable organization to make a real difference in our communities.

Who's Your Hero?

When you think "above-and-beyond community service," who among your CAP-member colleagues comes to mind? (Self-nominations are welcome.)

Please take a moment to share that person's story with us, then submit your nomination to

Communications@CAPphysicians.com.

Your nomination must include the name of the physician (CAP members only, please), and a statement that

identifies the charitable organization and summarizes the nature and scope of your nominee's service through that organization. We must receive your nomination statement no later than August 31, 2022.

If you have a nominee in mind who is not yet a CAP member, this is a great opportunity to make a referral! Please contact Membership Development at **800-356-5672** or **MD@CAPphysicians.com**.

A Win-Win for the Community

Our 2022 Community Hero Award recipient will not only receive personal recognition, but will also earn a \$5,000 grant for the associated charitable organization. One runner-up will receive CAP's Community Leadership Award, which includes a \$1,000 grant for the associated charitable organization.

All nominations will be thoroughly vetted, and winners will be selected by a team of CAP employees, the CAP Membership Engagement and Education Committee, and CAP's Board of Directors. We will announce the recipients of the Community Hero Award and the Community Leadership Award by December 31, 2022. Awards will be issued in January 2023. ↩

July 2022



Risk Management — and — Patient Safety News



From the Dark Side: The Alarming Rise of Violence in Healthcare

by Lee McMullin, CPHRM

In recent healthcare incidents and violent attacks that have swept the country, victims and their families have been left with unanswered questions as investigators attempt to piece together clues from the deceased suspects' social media posts, letters, and/or manifestos and determine the motives and patterns around their fatal and horrific actions.

If a perpetrator enters your doors with the intent to harm you or anyone in your practice, the motive for their violent behavior quickly becomes irrelevant, but your response does not. One thing is clear—don't leave the back door open.

On June 1st, 2022, a disgruntled patient entered a Tulsa, Oklahoma orthopedic office and fatally injured four individuals, including two physicians. It is unknown whether the practice had a threat assessment or response plan. The patient was upset because of ongoing pain following back surgery. Did the patient lack understanding about the potential surgical results? Did he have underlying anger issues? Did he have unrealistic expectations for what surgery could or would do for his condition? (Read more about managing patient expectations <https://www.capphysicians.com/articles/patient-expectations-root-all-evils>.) Regardless, the patient likely expressed anger to some degree at some point, but the office staff and/or physician may have lacked training and failed to appreciate the risk, or worse, dismissed the patient altogether.

This is not to say certain behaviors are precursors to threatening behaviors. It simply means "pay attention." There is a distinct difference between a patient with

residual back pain who is reasonably expressive about their condition and one who utters inappropriate comments or manifests dangerous behaviors.

Regardless of the behavioral signs, the reality is that physicians and office staff must:

- Develop a level of situational awareness to potential threats that may present, and;
- Create a pre-planned and rehearsed response.

Many medical offices are particularly vulnerable spaces simply by architectural design, with a reception area open to the public from either a hallway or outside airspace, and an open window or counter for patient check-in. However, there are actions you can take to improve the security of your environment.

Josef Levy, a retired Commander with the Long Beach Police Department and president and owner of Embassy Consulting Services, LLC., offers some practical tips for making medical practices a more secure work environment.

- Provide hands-on workplace violence/active shooter training, which is mandated by OSHA. Untrained staff will not be prepared or know how to respond to violence or an active shooter if it happens. Many people will default to duck and cover, which sadly, is the last thing they want to do. Training is critical and must be live and customized for your practice. Training should also include topics around the "Run, Hide, Fight-Active Shooter Protocol"; identifying "red flags" in patients or potential shooters; and stressing the importance of being vigilant. These

July 2022

are the most effective ways to deal with violence in the healthcare industry. History and statistics have told us that there are different and better outcomes for those individuals who have been trained in active shooter response versus those that have not been trained.

- Have an expert conduct a security site assessment of your office to identify vulnerabilities and make recommendations to create a safer work environment.
- TRAIN, TRAIN, TRAIN! Develop response plans, and regularly run practice drills. Implement an alert system, even if only a verbal shout to notify all of a threat. Situational awareness training—observing for threats and practical response patterns—will help you and your staff inside and outside of the office setting.
- Understand that office buildings are “projectile transparent” being made mostly of wall board affixed to thin metal studs. That means bullets will pass through and continue their trajectory until they strike solid resistance.
- Learn the difference between “concealment” and “cover”—concealment means you're hidden, cover means you're protected.
- Make note of patients and persons expressing or exhibiting inappropriate behaviors.
- Conduct morning huddles with all staff members to go over the day's events and any incidents involving inappropriate patient or individual behavior. If deemed by the office as a serious safety threat, staff should be made aware of the individual and provided with a physical description. However, caution should be taken to balance safety concerns with patient privacy rights and inappropriate profiling of individuals.

From a training perspective:

- There are several companies that offer general workplace violence prevention training, or AB508 Assaultive Behavior Management (ABM), either in person or online. AB508 ABM training is required for hospital staff working in certain high-risk areas. The length and costs of these programs can vary.

- Many local, state, and federal law enforcement agencies offer free online education for surviving an active shooter incident. Instruction manuals and YouTube videos, some as short as seven minutes, are available. Unfortunately, some of the videos are graphic, but they get the “Run, Hide, Fight” message across. Multiple resources are available by performing a quick internet search of active shooter training or prevention.

From a hardware perspective:

- **Door locks** - Is your pass door from the reception area to the back office secured? Can it be inadvertently left unlocked? Is it reinforced to resist being forced open from the reception area? This is where you want a solid, not hollow, door. Electronic locks work well when controlled from the reception area.
- Design your **reception area** to make it harder to enter the back-office area. Open air designs are attractive but make it easy for an attacker to jump over the counter.
- **A safe zone** - Do you have a designated area where staff can gather? A place that can be secured with a reinforced solid door? Your break room may be a viable option. An alternative is an escape method such as rear exit, especially one with quick access to stairs or the outside.

Active shooter situations and violence in the workplace and beyond are difficult topics to address, but it is better to be prepared before it is too late. If you're interested in having a security assessment of your office, please consult the CAP Marketplace at <https://www.capphysicians.com/practice-management/practice-management-services/cap-marketplace> under “Safety and Security”. ↩

Lee McMullin is a Senior Risk Management and Patient Safety Specialist for CAP. Questions or comments related to this article should be directed to LMcmullin@CAPphysicians.com

Gut and Amend: A Convenient Loophole in the Passage of AB 35

by Gabriela Villanueva



On May 23, 2022, Governor Newsom signed into law AB 35—a bill its proponents describe as the “Modernization of MICRA” (Medical Injury Compensation Reform

Act). Effective January 1, 2023, AB 35 codifies an annual increase in noneconomic damages (i.e., “pain and suffering”).

It is not unusual for the governor to sign a bill in the middle of a legislative cycle if the bill has gone through its customary course, but AB 35 had a different route—it had a swift passage through policy committee hearings and both Assembly and Senate floor votes by a mechanism legislators refer to as “Gut & Amend.” As the term suggests, “Gut & Amend,” is a quick, crafty method to advance a legislator’s bill.

AB 35 started its cycle like thousands of bills proposed by legislators at the beginning of the legislative two-year cycle in 2020. AB 35 was initially introduced by then Assemblymember Ed Chau in December 2020 with the intent of addressing false information on social media platforms. The bill was assigned to its committee hearings where the proposed language was completed and reviewed, voted on, and passed out of committee onto the Senate to proceed with a similar course of action. AB 35 continued its life as a social media bill until June of 2021, when it was scheduled for a Senate Judiciary Committee hearing. At this juncture, AB 35 stalled. It may have been because Assemblyman Chau resigned his seat after Governor Newsom appointed him as a Los Angeles County Superior Court Judge. The bill author was gone, but the bill was not.

Fast forward to April 27, 2022, when Senate Rule 26 was invoked and AB 35 now had a new author, Assemblywoman Eloise Gomez-Reyes. AB 35 was now

back in play—not as a social media bill, but rather a vehicle for proponents of MICRA “modernization” to introduce language to fundamentally alter the landmark statute.

Through the invocation and suspension of rules, the original content of AB 35 was removed—or “gutted”—and in its place, the new or “amended” language was entered. But why of all stalled bills in the cycle, was AB 35 the chosen one? In its previous form as a social media bill, AB 35 had already passed through the review, analysis, and committee hearing process in the Assembly. This meant that AB 35 only needed to make its way through the Senate to complete its journey. This process fosters very favorable conditions for a bill to swiftly pass without the traditional bill introduction, analysis, and hearing process.

With the freshly transplanted language written into a bill already slotted for a Senate Judiciary Committee hearing, AB 35 was out of its policy committee on May 3, 2022, and ready for a Senate floor vote. All rules pertaining to the 30-days public access to review the bill were suspended. On May 5, 2022, the Senate unanimously passed AB 35. It was then sent back to the Assembly floor for a concurrence vote on May 11, 2022. In less than a month’s time MICRA, a piece of legislation that has protected countless physician providers and their practices and has ensured the continued accessible options for care for over four decades, was itself gutted. Ultimately, the effect of passing AB 35, with such little consideration for serious analysis, thoughtful debate, and extended public review, will likely come at a very high cost. ↩

Gabriela Villanueva is CAP’s Government and External Affairs Analyst. Questions or comments related to this article should be directed to GVillanueva@CAPphysicians.com.



by Andie Tena

HIPAA Compliant Text Messaging: Doing More with Less Time

Practice staff are finding themselves with less time than ever before to complete day-to-day administrative tasks, including scheduling and confirming patient appointments. This is partially due to increased patient volumes and new administrative regulations, such as the No Surprise Billing Act that went into effect January 1 of this year.

According to a poll conducted by the Medical Group Management Association in May 2022, 50% of medical groups are seeing an increase in patient volumes over 2021, with 30% stating their volumes are equal to 2021 volumes. Patient demand combined with the “great resignation” of the last two years have left staff with more responsibilities, giving them less time to complete routine duties that are critical to the success and productivity of their practice.

How can practices optimize workflow while keeping costs down? The answer is simple. Implementing technology can help you and your staff work smarter, not harder. Here are five good reasons why implementing a HIPAA compliant text messaging solution may be a good start. You can:

1. Reach patients quickly - 95% of texts are read within 3 seconds, which allows you to reach out more effectively.
2. Reduce call volume by eliminating “phone tag” and leaving endless messages for patients.
3. Decrease no-show rates by engaging patients electronically for billing and appointment reminders.
4. Save staff time and improve efficiency - Utilize an automated system for the most common patient requests, appointment requests, refill requests, appointment confirmations, and patient check in.
5. Facilitate online reviews and generate a positive online reputation.

By leveraging technology to assist your practice in managing day-to-day tasks, you and your staff can focus on the most important assets in your practice, excellent patient care, and customer service!

For tips and resources on finding the right technology to help you improve efficiency in your practice, CAP members can take advantage of *My Practice*.

My Practice is a free member benefit offering practice management and business support to help you run a successful medical practice and spend more time focusing on superior patient care.

You or any of your employees may contact *My Practice* to get help with any practice-related challenges, no matter how big or small. Call **213-473-8630** or email **MyPractice@CAPphysicians.com** for immediate assistance. ↩

Andie Tena is CAP's Director of Practice Management Services. Questions or comments related to this column should be directed to ATena@CAPphysicians.com.

CYBERCRIME

Understanding Risk in Your Practice



Cybercriminals are no longer targeting only major companies with deep pockets—they are also going after small and medium-sized businesses.

Nearly half (43%) of cyberattacks are aimed at small businesses, yet only 14% of these businesses are prepared to defend themselves.* As criminals develop more awareness around security flaws, they are becoming increasingly sophisticated in their attacks, and without the proper infrastructure in place, your medical practice could be their next victim.

Top Threats to Cybersecurity

Ransomware attacks

Ransomware is a type of malware that denies a business's access into its systems and demands payment, for access to be regained. Payment is typically demanded by hackers through cryptocurrency, a credit card payment or untraceable gift cards. Although many companies are forced to pay the ransom in the hopes to minimize businesses losses, paying the ransom does not guarantee that a company will regain access. In fact, paying up may even make that company a target of future attacks, as cybercriminals often share details on the dark web about companies that pay ransoms.

Ransomware enters a company's system in a variety of ways, but the most common is through target emails. These messages include a link to a malicious website, and when the user opens the infected attachment,

ransomware contaminates the victim's computer and quickly multiplies throughout the network—crippling operations.

COVID-19-related threats

The recent COVID-19 crisis brought on a "cyber pandemic" as criminals discovered new ways to take advantage of vulnerabilities and gain access to systems. From ransomware to data breaches to unemployment fraud, COVID-19 has accelerated existing challenges and unleashed an entirely new set of obstacles. Healthcare remains a vulnerable, popular target among cybercriminals as hackers hold valuable patient data and networks hostage until the companies meet their demands. North American companies are notably more likely to be targets of these attacks, experiencing 117% more attacks than Europe.

Accessing open RDP ports

Hackers are developing new ways to get access to networks by detecting Remote Desktop Protocol (RDP) ports. RDP ports enable employees working away from their physical office to access computers and stay connected through remote work. This connection method has become more commonplace and is essential for many businesses, but open RDP ports can leave vulnerable pathways that allow hackers to cause irreversible system damage.

If a criminal can dig deeper within the system, they oftentimes corrupt backups of all files, leaving the

business with no alternative but to pay the ransom to access their systems and data and reduce the amount of downtime for their business.

Entering an RDP port oftentimes solely requires that the cybercriminal uncovers a set of login credentials. Threat actors steal these login credentials on their own or purchase them on the dark web.

Many cybercriminals are also gaining access to critical data within systems through the cloud. Organizations have adopted cloud applications, especially during the pandemic to enable remote working, and criminals quickly found ways to exploit weaknesses.

Additionally, criminals are creating targeted attacks to managed service providers (MSPs), which are companies that manage a customer's IT infrastructure or other systems. Hackers targeting MSPs use unauthorized access to deploy ransomware attacks on multiple client environments, leading to an aggravated event from one compromised system.

Top Cybersecurity Misconceptions

1. My data isn't valuable enough

All organizations have valuable data that is worth protecting, and cybercriminals are targeting Service Message Blocks (SMBs).

2. I'll know whether my organization has been breached

Cybercriminals are talented at covering their tracks. And the longer they stay inside your system, the more damage they will do.

3. Cybersecurity is a technology issue

Cybersecurity is the responsibility of every part of the organization, not just the IT department.

4. Outsourcing to a vendor ensures that we're safe

There are many cases of MSPs being targeted, so it's critical to ensure that any partners you work with have robust cybersecurity measures in place.

5. Cybersecurity breaches are covered by my general liability insurance

Most standard liability insurance policies don't cover these types of threats. Speak with your insurance broker to understand the coverages available.

Should You Pay the Ransom?

The FBI doesn't support paying cybercriminals the requested ransom because doing so encourages the business model. Additionally, adversaries may publicize that information on the dark web—making you a future target. Less than half of ransomware victims that pay the ransom can successfully restore their systems.

Mitigation Strategies

The number of cyberattacks taking place every year is surging, and organizations need to take adequate precautions to prevent these attacks before they suffer irreversible harm.

• Build a stronger backup strategy

The configuration of backups is critical. Attackers are likely to delete backups prior to deploying ransomware to increase the odds that you will pay. Oftentimes backup strategies are designed to protect against hardware failure, but they weren't designed to protect against hacker infiltration. Up to 40% of ransomware claims have affected backups. Purchase a backup solution that uses a separate non-domain account with multifactor authentication. Retain multiple copies of data and keep one offsite. Closely monitor your backup solution for suspicious activity and data exfiltration.

• Use multifactor authentication


Improve your security posture by requiring a multifactor authentication on all public-facing employee service protocols. Also, restrict internet-facing protocols, such as Remote Desktop Protocol and Server Message Block, to help prevent unauthorized access to your environment.

• Implement a stronger endpoint solution.

Use advanced endpoint protection across your network. These solutions should use machine learning to spot potential challenges in addition to conducting

antimalware and antiviral activities in real time. The solution should be capable of detecting and preventing unknown threats and detecting unmanaged assets within the corporate environment.

With threats moving at a faster and even automated pace, speed will be critical for businesses attempting to stay ahead of criminals. Medical practices need to develop strategies, and then frequently and rigorously test those strategies, so that they will be ready when cybercriminals target their organization.

The licensed professionals with CAP Physicians Insurance Agency (CAP Agency) can help you learn about your own personal cyber risk and about affordable coverage options and services available through Tokio Marine HCC. For more information, please contact CAP Agency at **800-819-0061** or email **CAPAgency@CAPphysicians.com**. 

The information in this article is provided by Tokio Marine HCC. Tokio Marine HCC is the marketing name used to describe the affiliated companies under the common ownership of HCC Insurance Holdings, Inc., a Delaware-incorporated insurance holding company. Headquartered in Houston, Texas, Tokio Marine HCC is a leading specialty insurance group with offices in the United States, the United Kingdom, and Continental Europe.

*<https://www.cnn.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html>



CAP PHYSICIANS INSURANCE®
License No. 0F97719

Save
the Date

The Truth Behind AB 35 and Its Impact on California Physicians

Presented Through the 4th Annual Public Affairs Symposium

Virtual Program | Wednesday, September 21, 2022 | Noon-1:30 p.m.

On May 23, 2022, Assembly Bill 35 (AB 35) was signed into law by Governor Gavin Newsom. AB 35 significantly increases the caps on noneconomic damages and attorney's fees in medical malpractice lawsuits, diminishing the important protections and limits provided by MICRA—the Medical Injury Compensation Reform Act of 1975.

AB 35 will pose significant challenges to the medical community for a variety of reasons as a surge in malpractice claims frequency and severity is expected after the law goes into effect on January 1, 2023.

CAP members are invited to participate in our 4th Annual Public Affairs Symposium where a panel of legislative experts and policy analysts will provide a behind-the-scenes look at how AB 35 materialized, explore what the legislation means for your medical professional liability risk, and discuss what you can do to protect your practice.

The symposium is a free virtual event exclusive to CAP members. Registration details will be available soon.

For more information, please contact **PACinfo@CAPphysicians.com** or call **213-473-8762**.

July 2022

Case of the Month



The (Very) Thin White Line— When We Exceed Safe Speed Limits

by Dona Constantine, RN, BS
and Lee McMullin, CPHRM

We've all heard the term "speed kills." Just like a road or freeway is engineered with consideration of vehicles in motion towards an established maximum safe speed, the medical office, too, is designed for efficient, safe care at a maximum limit. When those limits are exceeded, there is a proportionate relationship to speed and risk of patient harm. Just like weather affects the safety of a roadway, the "weather" in the medical office likewise must be assessed on an ongoing basis to know if you can "punch the throttle" or slow down—there may be hazards ahead, as the following case illustrates:

In August 2013, an employee reported to his employer's designated workers' compensation health center after being injured. The employee, now the patient, presented to the health center for evaluation of right leg, lower back, and elbow pain. A physician assistant (PA) student documented the patient's history of diabetes, obesity (BMI 32), arthritis, and consumption of Advil. The health provider ordered lumbar spine and right knee X-rays. After reviewing the results, the provider diagnosed the patient as having a lumbar spine strain, right knee and elbow contusions, and severe back and knee arthritis. The patient was discharged with prescriptions of Vicodin and Ibuprofen.

For several months, the patient continued to be seen at the health center for his back and leg pain. During this time, the patient was seen almost exclusively by

PA's until he was cleared by an orthopedic physician for surgery. Despite the patient's fear of surgery, he elected to undergo a lumbar decompression to alleviate his continuing pain. Surgery was performed without any intraoperative complications. However, the patient's post-operative course was wrought with infection and wound healing issues. An infectious disease (ID) specialist was consulted and opined that the patient most likely had a polymicrobial infection due to Arava, an immunosuppressive medication, which inhibited wound healing. There was no prior documentation in the medical record that the patient had been taking Arava. The ID specialist discontinued the Arava and initiated an aggressive poly antimicrobial therapy. Although the patient's condition initially improved, he later succumbed to sepsis.

The patient's family filed a wrongful death action alleging the failure to discontinue Arava as a cause of the uninhibited infections that ultimately resulted in death. The matter subsequently resolved informally prior to trial, yet there are several points to be considered in the outpatient management of this case:

Review of Prior Health Records

When the patient first presented to the health clinic in October 2013, a more thorough evaluation of the patient's health history records would have revealed that the patient had rheumatoid arthritis (RA) and was

taking Arava. This same entity who provided care to the patient for his work injury had also performed the patient's pre-employment examination. The patient's history of RA and use of Arava is documented in the prior records which were in the clinic's possession.

Supervision of PAs and Student PAs

A student PA obtained the patient's medical history during his October 2013 visit. The medical history documented by the student was simply "arthritis," with no mention of the type of arthritis, in this case, RA. Further questioning of the patient regarding his arthritis may have elicited he was taking the immunosuppressant medication Arava, in addition to the Advil that was reported. Additionally, since the patient was almost exclusively seen by PAs until cleared for orthopedic surgery by a physician, the adequacy of PAs and student PAs comes into question.

Too many clinics, too many patients

The workers' compensation provider operated several clinics whose staff performed 10,000 pre-employment physicals each month in addition to managing injured worker healthcare caseloads. With high patient volumes, it could be construed that students were managing patient volumes beyond the scope of licensed staff. An overriding concern is whether the clinic's volume exceeded its capacity. Were staff "speeding" and processing patients too fast, and not taking the time to investigate matters further? If your bandwidth that day is only allowing for one lane of traffic, then try closing the other three lanes to manage the current conditions. For example, maybe you have several staff members out and cannot manage the flow. Remember that the collisions that take place become your liabilities. If you need to use students to manage patient volumes beyond the scope of licensed staff, you're speeding. If you have a patient traffic jam every day in your office, you're not managing the traffic. Patient safety starts with the onramp of your office and doesn't stop until they exit.

Medical Record Systems and Documentation

Handwritten paper medical records were used by the clinic when the patient was initially seen for his pre-employment exam. This is a daunting record-keeping system considering the huge patient volume seen by the clinic staff. Prior to the patient's injury and surgical evaluation, the clinic transitioned from paper charts to an EHR. The patient's history of RA and immunosuppressant medication history was not uncovered and carried over to the EMR. Consequently, this information was not in the records reviewed by the surgeon who cleared the patient for the lumbar decompression.

Several system issues in the outpatient management of this patient may have contributed to the failure to communicate pertinent information to the operating surgeon, and discontinuation of the Arava prior to the spinal surgery.

The case illustrates the dangers to patient safety with a "herdlike" approach to patient volume. With a focus on maintaining patient volumes and throughput, there can be a tendency to overlook the safety variables inextricably interwoven which exceed the limits of safe patient-to-provider volumes. Is safety being sacrificed by staff and providers to meet certain metrics or incentives?

The moral of the story is that a medical practice needs its own internal "highway patrol," as a lack thereof will be gladly taken up by plaintiff lawyers and the medical board. ↩

Dona Constantine is a Senior Risk Management and Patient Safety Specialist for CAP. Questions or comments related to this article should be directed to DConstantine@CAPphysicians.com.

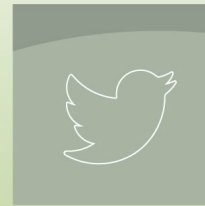
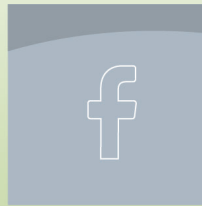
Lee McMullin is a Senior Risk Management and Patient Safety Specialist for CAP. Questions or comments related to this article should be directed to LMcmullin@CAPphysicians.com



COOPERATIVE OF
AMERICAN PHYSICIANS

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

Connect with CAP on Social Media!



IN THIS ISSUE

- 1 Celebrating Our CAP Community Heroes:
A Call for Nominations!
- 2 Risk Management and Patient Safety News:
From the Dark Side: The Alarming Rise of Violence in Healthcare
- 4 Public Policy:
Gut and Amend: A Convenient Loophole in the Passage of AB 35
- 5 Ask My Practice:
HIPAA Compliant Text Messaging: Doing More with Less Time
- 6 CYBERCRIME Understanding Risk in Your Practice
- 8 Save the Date: CAP's 4th Annual Public Affairs Symposium
- 9 Case of the Month:
The (Very) Thin White Line – When We Exceed Safe Speed Limits

July 2022

Copyright © 2022 Cooperative of American Physicians, Inc. All rights reserved.
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.

The information in this publication should not be considered legal or medical advice applicable to a specific situation.
Legal guidance for individual matters should be obtained from a retained attorney.