THE MONTHLY PUBLICATION FOR CAP MEMBERS

CAPsules®

COOPERATIVE OF AMERICAN PHYSICIANS
CELEBRATING 40 YEARS OF SUPERIOR PROTECTION

Cyber Security: A Critical Risk Management Issue for Your Practice

by Tom Andre

The healthcare industry faces a growing risk from cyber attacks, which makes it critical for CAP members to devote sufficient resources to designing and implementing a strategy that can mitigate that risk.

The internet is a medium that offers many benefits. It provides easy access to useful resources and to people around the world. At the same time, criminals across the globe have unprecedented access to us. Recent events have shown that healthcare organizations can be severely impacted by cyber attacks.

It can be discouraging to learn that large organizations like Sony and Target are victims of these attacks. After all, if firms with large security budgets and staff cannot avoid them, how can a much smaller organization?

It also may be tempting to think that an individual or small organization has little value to attackers and is thus an unlikely target. Ransomware attacks of recent months are evidence to the contrary. Criminals have received millions in ransom payments from individuals as well as from small organizations.

Cyber security experts agree that no organization can prevent every possible attack. It is still important to take steps to reduce your security vulnerabilities. You should also be prepared to respond to and recover from an attack. You may not experience every possible type of attack, so your immediate focus should be on addressing the types of attacks most likely to affect you.

Here are some suggestions:

Keep all of your machines "clean." As recommended by the National Cyber Security Alliance and others, this means keeping software on all Internet-connected devices up-to-date. Install updates and security patches as soon as possible.

Hackers stole personal information on 143 million U.S.

consumers from Equifax in May. In that same month, a ransomware attack crippled the U.K.'s National Health Service. A large hospital chain in the U.S. had a similar ransomware incident last year. What do they all have in common? Hackers exploited software vulnerabilities. In all three cases, a patch had been available for weeks, but was not installed.

So, if you thought you couldn't do better on cyber security than a large organization, here is an area where perhaps you can.

continued on page 2

December 2017

Continued from page 1

Backup often and maintain offline copies of backups. Many ransomware victims are able to recover without paying the demand because they are able to obtain damaged files from backup. However, be sure that if one of your computers is infected with ransomware, it can't reach and compromise the backup data, or any computer connected to the backup data.

Keep your "human firewall" up to date. Phishing and social engineering are among the most prevalent attacks against small and medium-sized organizations. This means that email programs and web browsers are major conduits for malware delivery. Firewalls, spam filters, and anti-malware software all play a part in protecting against this. But cyber crime is lucrative. Attackers change tactics to avoid these counter-measures. Malware propagation by phishing and social engineering relies on exploiting human as well as technical weaknesses.

Consider cyber security awareness training for yourself and for employees who use email or browse the web. Informed people who understand attacker tactics can be an effective last line of defense. For example, simply taking a moment to examine an email for suspicious indicators before opening an attachment or clicking a link can avoid having to clean up a cyber mess.

Use current malware defenses. Antivirus and malware products have changed and are still evolving. "Old-school" antivirus programs relied on the vendors identifying their unique pattern or signature, and publishing that information for its clients. This approach already had a built-in flaw. Your computer could be infected if you received the malware before the vendor discovered it and published an update. Attackers are now developing malware that regularly changes the signatures, making it more difficult to identify. Newer products ("next-generation antivirus") still recognize signatures. In addition, they use machine learning techniques to identify unusual behavior. Check your antivirus product to see if it includes such advanced capabilities.

Protect your email account. Email services are often free (Google, Yahoo, AOL, etc.). While the cost may be trivial, the value of your email account can be significant to you and an attacker.

If someone gained access to your email account, what could they find that is valuable? Your address book? Would you want phishing messages sent to friends and associates from your email account?

Do you have accounts with online merchants and services? Consider this scenario: A hacker takes control of your email account and discovers (from your emails) that you are an Amazon customer. The hacker can go to Amazon's website, enter your email address, and click "Forgot Password." Amazon will send a password reset link to your email, which the hacker now controls. If you have credit cards saved in your account, the hacker can login and make purchases.

Exercise care with your email credentials. It is okay if you go directly to the mail provider's website and log in. But be wary if you find yourself directed to a login page after clicking on a link in an email or an attachment. The page may look like your email service. But check the address (URL). Some prominent national figures have had their email accounts hacked in this way.

If your email service offers it, consider using two-step verification. This generally involves entering a code that is sent to your mobile phone, or provided in an automated voice phone call. So even if someone obtains your password, they cannot login without physical access to your phone. This is also a good idea for any other online accounts that you want to keep safe.

Keeping computers safe is an ongoing challenge. Attacker tactics change constantly. So it is important to maintain an awareness of the latest threats and countermeasures. Fortunately, there are many online resources available for help. One good place to start is the National Cyber Security Alliance - StaySafeOnline.org.

Tom Andre is CAP's Senior Vice President, Information Services. Questions or comments related to this article should be directed to tandre@CAPphysicians.com.

Hold the Phone! Risk Management Insights into the Perks and Pitfalls of Our Favorite New Mode of Communication: Text Messaging

The ease, efficiency, and utility of text messaging isn't lost on healthcare professionals, 90 percent of whom use it as a method for sharing information with colleagues, patients, and staff. Although text messaging may be our new preferred mode of communication, enthusiasts are well advised to momentarily put down their mobile devices and educate themselves on the existing legal restrictions, the emerging best practice recommendations, and the unique rules that currently govern provider-provider and provider-patient text messaging.

Rules and Recommendations for Provider-Provider Text Messaging

In December 2016, The Joint Commission issued a clarification statement establishing the following limitations on text messaging between providers:

► Unencrypted text messaging of communications that include PHI is prohibited.

The standard short message service (SMS) that conveniently exists on your mobile device is considered a prohibited, unsecure texting platform—making all communications transmitted via this medium vulnerable to hacking, unauthorized access, and a HIPAA violation. The Office of Civil Rights regards the use of an unencrypted text messaging service for the communication of PHI as a HIPAA breach. The fines for a breach of HIPAA can be quite high. The fine for a single breach of HIPAA can be anything up to $50K per day if the vulnerability responsible for the breach is not attended to.

► Here are a few examples that were found to be HIPAA violations while sending unencrypted text messages:

1. A doctor texted an MA (on MA's personal mobile phone) asking the MA to text him the lab results for a patient the physician was planning to see in the hospital that day. Unbeknownst to the physician, the MA was not scheduled to work that day. Fortunately, the MA had her phone with her and called the office to ask a coworker to contact the physician with the lab results. Neither the doctor nor the MA had text messaging encryption.
2. A doctor asked a staff member to *take a picture* of the most recent progress note from a treating specialist and to send the picture of the specialist's report to the doctor's unencrypted phone.
3. An office manager routinely scans patient EOBs and then texts the scanned information, unencrypted, to the outside biller.
4. Doctors and staff frequently text with patients about appointments, medical conditions, and medication questions and think they are HIPAA compliant as long as the patient chooses this mode of communication despite being unencrypted.

Over the last few years, more medical professionals have come to rely on their personal mobile devices to support their workflows. However, because so many healthcare professionals are using mobile devices, there is a considerable risk that PHI may be accessed by unauthorized people. This occurs because most apps and mobile devices do not require a log-in or log-out and, therefore, if the device is lost or stolen, the PHI stored in the device would be easily accessed and released to unauthorized individuals.

continued on page 4

Continued from page 3

So, while it's perfectly acceptable for staff to use an unencrypted texting service for messages such as, *"Doctor, you have patients waiting,"* a text that includes a patient's protected health information, *"Mary Smith's INR is 7,"* would be considered a HIPAA violation.

The bottom line? If you're texting your office staff, your colleague, the hospital nurses, sending photos, films, videos, reports, or communicating *any PHI relating to a specific patient's care* – ***encrypt!*** Understand that attempts to circumvent encryption by masking the identity of a patient (using abbreviations or referring to a patient by location) can easily backfire and result in adverse events caused by patient misidentification. Also, physicians in private practice should understand that if their policy is to utilize unencrypted text messaging for practice management purposes only, there must be adequate education and training of staff to reinforce permissible versus impermissible texting content.

The Joint Commission has made several attempts to adopt a policy that will ensure a safe implementation of text messaging in healthcare. The Joint Commission is encouraging healthcare providers to develop policies and educate staff on the limitations of unsecure texting in the workplace. These might include:

- An inventory of all mobile devices used for texting ePHI (whether provider-owned or personal);
- Proper sanitization of mobile devices that text ePHI upon retirement of the device;
- Policies that prohibit or limit the type of information that can be shared via text;
- Training on the appropriate use of work-related texting; and
- Password protection and encryption for mobile devices that create, receive, or maintain text messages with ePHI.

Texting *orders* is prohibited, even if secure.

Years ago, The Joint Commission established standards limiting the use of verbal orders to situations where a written order was either impossible or impractical. The Joint Commission recognized that verbal orders imposed a substantial clerical burden on nursing staff and also increased the potential for error by inserting yet another fallible human in the order entry process.

The Joint Commission likens text orders to verbal orders, with a few additional risks. Like verbal orders, text orders require nurses to transcribe orders into the EHR, adding to their clerical burden and increasing the likelihood for error. Additionally, as text messaging is an *asynchronous interaction*, it prevents nurses from being able to obtain immediate clarification on a text order or to respond instantly to Clinical Decision Support (CDS) alerts and recommendations — leading to further delays in care. Finally, there is no way to preserve original text documentation as validation of what was ordered.

CAP Risk Management and Patient Safety department recommends that members incorporate provider-provider and provider-patient text messages with clinical information into the medical record. From a defense standpoint, CAP data support the following defense challenge – but for the missing documentation of a telephone call or the text message, the case would have been dismissed or easier to defend.

Barry B. Cepelewicz, MD, JD, a contributing writer to *Medical Economics*, stated "Any text message that involves the transmission of information that would be considered PHI, including information relating to the treatment of your patients, should be considered part of, and therefore incorporated into, your medical record. Most physicians would readily agree that a letter from a patient describing a medical condition or correspondence from another treating physician offering treatment recommendations should be included in the medical record, and that a conversation relating to a patient's care should be memorialized in the record."

From a professional liability perspective, you would not want to put yourself in a position where a patient suing you for malpractice can make claims that hinge on various text messages between you and the patient, and you did not retain copies of those messages.

Authored by members of the CAP Education Committee – Hospital Education Subcommittee. A special thank you to Catherine Miller, JD, RN and to Jeffrey Shapiro, MD for their contribution to this article.

Ransomware Attack – A CAP Member's Story

by Jeff Mongelli

Like the fable about the boy who cried wolf, we so frequently hear about this or that threat, that we simply become numb to the noise and ultimately turn a deaf ear. Sadly, our tendency to ignore all but the immediate dangers is an approach that's being exploited by cyber hackers. Ransomware is evolving, growing, and becoming increasingly sophisticated and effective.

In a recently published survey of IT firms, including Acentec, Inc., we were asked about our clients' experience with ransomware in 2016.* What they reported is startling.

91% of the firms surveyed reported recent ransomware attacks on their clients.

100% reported increasing frequency of attacks.

93% of ransomware evades antivirus and anti-malware detection.

Healthcare is the second most targeted industry.

Recently, we reported in one of our free weekly HIPAA security reminders an attack called "Bad Rabbit." This month, the healthcare industry is experiencing highly targeted email phishing schemes. A typical example is you receive an email from a referring physician, with an attached PDF, Word, or other document; a seemingly routine email. However, the sender had been compromised by a virus that sends out reply emails to existing contacts. Once triggered, your files are encrypted, your systems locked, and your monitor displays the dreaded ransomware threat – pay us or we'll delete your data.

Just such a situation has happened to numerous CAP physicians. Here's one member's story:

"A member of our staff opened an email one day, and moments later, we were all locked out of our computers with a red screen saying we need to pay them to get back into our system. We immediately called our IT company. They eventually had to wipe out all of our computers and restore everything from backups. We were down for two days and had to cancel patient appointments as they arrived, since we didn't have any records. In the end, we lost a week's worth of data, and had some fairly upset patients. Although it was not a HIPAA breach, we did report it to the FBI."

What can you do to avoid being added to the growing victim list? Train your staff to be aware and stay aware. The majority of attacks are coming through emails. Here are some general rules:

- Don't click links in emails. Instead, open a web browser and go directly to the site.
- Don't open email attachments. If you receive an email with an attachment, call the sender to confirm they sent it.
- If you did open an attachment and it asks you to enable something, *don't*.
- Lock down your network to scan for threats at the firewall. Call us if you need help with this.

Finally, accept that despite your best efforts, you may still get attacked. If that happens, you have two options – pay the ransom, or wipe your system and restore from backup. The FBI advises to never pay the ransom since there's no guarantee you'll get your data, and many don't. So you're left with restoring from backup. If you don't have a business disaster recovery device (BDR), put it on Santa's wish list and make a New Year's resolution to implement one in 2018. A BDR will eliminate downtime, lost data, and it could very well save your practice and your reputation.

* Survey conducted by Datto of 1,100 leading IT firms in the country.

Jeff Mongelli is CEO of Acentec, Inc., a nationwide provider of HIPAA compliance and medical IT management services. If you have any questions about this article or would like recommendations, please contact him for a free consultation at 800-970-0402 or jeffm@acentec.com.

December 2017

New California Healthcare-Related Laws for 2018

Once again, it is time to look ahead to the new year and learn about the incoming set of new laws to take effect starting on January 1, 2018, or at some point during the year.

At the end of the 2017 legislative calendar, Gov. Jerry Brown vetoed only 118 of the 977 bills that came to his desk — one of his lower veto rates in recent years. This leaves all Californians with 859 new laws on the books. Of the close to 50 healthcare-related bills that became law, below are some of the highlights.

► **Medical Board of California.** The Medical Board of California, established under the Medical Practice Act for the licensure and regulation of physicians and surgeons, has been extended another four years. Existing law requires the Governor to appoint members to the Board, authorizes the Board to employ an executive director, investigators, legal counsel, medical consultants, and other assistance, and requires the Attorney General to act as legal counsel for the Board. In signing SB 798 extending the Board's sunset date, Gov. Brown said: "To the Members of the California State Senate: I am signing Senate Bill 798, which extends the sunset for the Medical Board of California and the Osteopathic Medical Board of California from January 1, 2018, to January 1, 2022. Two issues were identified during the legislative process requiring further review: vertical enforcement and the exchange of expert witness reports between a doctor under investigation and the Medical Board. I am directing my staff to work with the Legislature and the Attorney General's Office to determine what changes are needed."

► **CURES:** The Controlled Substances Utilization Review and Evaluation System (CURES) remains a tool for legislators as the opioid crisis continues to generate national attention. Under AB 40 to be in effect no later than October 1, 2018, the State Department of Justice shall authorize a healthcare practitioner or pharmacist to submit a query to the CURES database through the department's online portal or through a health information technology system if the entity operating the system has entered into a memorandum of understanding with the Department addressing the technical specifications of the system and can certify, among other requirements, that the system meets applicable patient privacy and information security requirements of state and federal law.

► **Filling a Partial Scheduled II Controlled Substance:** Beginning July 1, 2018, a pharmacist will be authorized to dispense a Schedule II controlled substance as a partial fill if requested by the patient or the prescriber. AB 1048 will require the pharmacy to retain the original prescription, with a notation of how much of the prescription has been filled, the date and amount of each partial fill, and the initials of the pharmacist dispensing each partial fill, until the prescription has been fully dispensed.

► **Creation of a New Fellowship Program in Mental Health:** The Mental Health Services Oversight and Accountability Commission is authorized under AB 1134 to establish a fellowship program to provide an experiential learning opportunity for a mental health consumer and a mental health professional.

continued on page 7

Continued from page 6

The bill requires the Commission to establish an advisory committee to provide guidance on the fellowship program goals, design, eligibility criteria, and application process. The bill authorizes the Commission to enter into an interagency agreement or other contractual agreement with a state, local, or private entity, and to receive technical assistance or relevant services to support the establishment and implementation of the fellowship program.

► **Genomic Cancer Testing Information:** Current law requires a physician and surgeon to give a breast cancer patient a standardized written summary, made available by the Medical Board of California with recommendations from the Cancer Advisory Council, to inform the patient of the advantages, disadvantages, risks, and descriptions of the procedures medically viable and efficacious alternative methods of breast cancer treatment. The summary is required to be revised every three years and include any new or revised information. AB 1386 requires the State Department of Health Care Services to include information relating to breast cancer susceptibility gene (BRCA) mutations, in order to achieve increased genetic counseling and screening rates of individuals for whom BRCA test results can inform treatment decisions.

► **Temporary Expansion of Scope of Care:** The California Hospice Licensure Act of 1990 provides for the licensure and regulation by the State Department of Public Health of persons or agencies that provide hospice. SB 294 authorizes, until January 1, 2022, a licensee under the Act to provide any of the authorized interdisciplinary hospice services, including palliative care, to a patient who has a serious illness. The bill would require a licensee who elects to provide palliative care pursuant to this temporary authorization to report additional specified information to the Department, including the number of patients receiving palliative care.

The California Legislature returns for the 2018-2019 legislative session on January 2, 2018.

Bill information language was provided by Lindsay Gullahorn, Legislative Analyst at Capitol Advocacy in Sacramento.

Want to Improve Your Cyber Fitness? Free Online Courses Will Show You How!

As a CAP member, you automatically receive cyber risk protection though NAS Insurance Services to help protect you against information data breaches, including HIPAA.

We are happy to report that NAS has recently launched an online tool called CyberNET, that offers CAP members and their staff free access to a number of training courses to help keep you HIPAA compliant and reduce the likelihood that you'll fall victim to a cyber attack. These courses include:

- Introduction to Breaches
- Data Security Basics
- Social Engineering
- HIPAA Training Series (with printable certificate)
- Safeguarding Information
- Payment Card Industry – Identifying Fraudulent Payment Cards

This new site also enables you to directly report a breach to NAS, as well take the Cyber Risk Fitness test to find out just how vulnerable you may be.

To access CyberNET: visit the CAP website at CAPphysicians.com, go to the "Risk Management" page, then click on **CyberNET HIPAA Training**. First-time users will need to register using your CAP member number as your sign-up code.

Also be sure to call CAP Agency at 800-819-0061 or email CAPAgency@CAPphysicians.com to learn about your current cyber risk coverage and how you can increase your limits so you're well-protected in the event of a breach.

CAP PHYSICIANS INSURANCE®
License No. 0F97719

The Successful Physician

by Carole A. Lambert, MPA, RN

Telehealth – Patient Care, Practice Growth, and Cyber Risks

To quote *Becker's Hospital Review*: "Telehealth is one of the fastest growing solutions implemented across major health systems today. Healthcare providers face considerable challenges in care delivery and will require targeted strategies and solutions to extend care access, improve quality, and lower costs." *Becker's* further notes statistics from one single telehealth provider, Teladoc in Lewisville, Texas: "In 2016, Teladoc shared insights gained from facilitating their first 1 million telehealth visits. Since then, Teladoc has now facilitated over 3 million telehealth visits…." Evan Sweeney in *FierceHealthcare*, cites a report from the Center for Connected Health Policy noting that 48 states and Washington, D.C. reimburse for live telehealth video visits and 15 allow payments for store-and-forward technology.

What great opportunities to reach people in need and provide access to quality care while containing costs! What mind-bending chances for gaps in security and privacy! Ashley Blume in HealthIT Security notes that: "… even though telemedicine has much to offer healthcare providers, they must think carefully when making the decision to incorporate it into their practices because there are security risks… Healthcare providers need to ensure that their patients' ePHI is secure and encrypted to prevent a data breach or cyberattack."

At the organizational level, Alan Hille of Ultra Risk Advisors offers five tips for reducing cyber security risk in telemedicine:

1. Appoint a HIPAA security officer and conduct a data security self-assessment.
2. Develop and implement action plans for gaps identified in the self-assessment.
3. Implement safeguards across the continuum.
4. Audit contracted teleradiology providers.
5. Establish policies and procedures related to data security.

Michael T. Blatt and Elizabeth Callahan-Morris offer considerations and recommendations on "Pitfalls and Benefits of Telehealth and Cybersecurity in the Digital Age." The general areas of risk that Blatt and Callahan-Morris identify include electronic medical records, mobile devices, medical devices, and web-based applications. Blatt and Callahan-Morris get down to security fundamentals with risk analysis; policies and procedures; training; sanctions; and documentation. In regard to telehealth specifically, they note legal considerations such as HIPAA, credentialing, licensing, and medical professional liability, among others.

Then there are the elements of the clinician-patient relationship and the standard of care. These include patient identification, clinician identification (MD, PA, APP), informed consent, a thorough assessment to facilitate diagnosis and the development of a treatment plan, and follow-up care. Documentation is, as always, the key to communication among members of the healthcare team from the patient and family to the treating clinician to the referring clinician to the pharmacy to the billing entity to the payer and to medical-legal challenges.

Simple arithmetic doesn't capture the numbers of prospects for trouble as patient encounters, devices, clinicians, employees, and cyber attackers multiply – they are exponential. However, the areas of risk are familiar and may be addressed with attention to, and focus on, equally familiar strategies. We can mobilize security tools to help manage these areas of risk, but our investment will always encounter what The Joint Commission calls the "human factor."

continued on page 9

Continued from page 8

As we implement and increasingly use telehealth capabilities, we must commit to acknowledging the implications of this approach to patient care. The foundation of success with telehealth is rigorous documentation standards. We must commit to monitoring risky behavior; consistently applying policies and procedures for appropriate use; staying up-to-date with hardware and software iterations; and to insisting on appropriate clinician and staff behavior. Our understanding of the risks associated with telehealth is the vital first step in creating cyber security and mitigating cyber risk.

Carole A. Lambert is CAP's Vice President, Practice Optimization. Questions or comments related to this article may be sent to clambert@CAPphysicians.com.

Improving Healthcare Delivery and the Patient Experience Through Videotaping

Do you find yourself asking, "How can I give my patients more time when there are just not enough hours in the day?" or "How can I better communicate critical information to not only to my patients, but involved family members as well?" Randall Porter, MD, founder of CAP's new CAPAdvantage program provider, Medical Memory, asked himself these same questions – not only as medical practitioner, but as a son helping to care for his out-of-state father diagnosed with cancer.

This frustrating experience as an out-of-area family member led Dr. Porter, a neurosurgeon at the Barrow Brain and Spine (BB&S) in Phoenix, to launch Medical Memory – healthcare's first enterprise cloud-based video patient engagement solution.

"I knew immediately how inefficient it was for physicians and their staffs to have the same conversation over and over again. I realized that a better, more efficient process would involve a video of doctor/patient consultations," said Dr. Porter. And the results are proving him correct.

According to Julie Supple, ANP-BC at BB&S, "Our team has seen a significant reduction in post-visit phone calls from patients requesting more information about '…what the doctor said'." Dr. Porter's team at BB&S evaluated 400 patients: half of whom had clinical recordings of their visit and the other half did not. The outcome was significant, showing a **25 percent reduction in the number of follow-up phone calls from the patient group that had access to their clinical recordings**." That's 200 happier, more informed patients and 50 fewer post-visit phone calls where staff has to locate the care team, or pull and review a chart to answer the patient's question.

Clinicians are also utilizing pre-recorded content to improve efficiency and the quality of the time spent interacting with the patient. According to Deborah Shepard, ACNP, at Barrow Brain and Spine, "We end up repeating the same things multiple times per week, such as post-operative instructions. We have found it much more impactful to have the patient watch pre-recorded, post-operative instructions where we know all of the generic instructions are covered 100 percent correctly every time. Then when the patient is done viewing that video, we come in and talk about the more personalized instructions important to that patient's care."

To see for yourself how this HIPAA-compliant videotaping platform can improve your practice efficiency and the patient experience, **Medical Memory is pleased to offer CAP members a free 60-day trial.** For more information visit www.themedicalmemory.com/cap-physicians, call 855-500-0051, or email CAP@themedicalmemory.com.

Case of the Month

by Gordon Ownby

Getting the Attention of Your Wandering Patient

Physicians and their staffs have a hard enough time getting their patients to understand the urgency of undergoing follow-up testing. When the condition looks serious and a frequently traveling patient has a history of noncompliance, getting him or her to a specialist – or to the ER – may be what's called for.

A 48-year-old gentleman whose business frequently required world travel had high blood pressure, high cholesterol, and a family history of heart disease. Between his initial visit with his internist, Dr. IM, for a sleep disorder and his final visit seven years later, the patient showed a propensity of not adhering to his blood pressure medication regimen. Midway through that period, Dr. IM prescribed a statin for high cholesterol.

During a work project, the patient's schedule took him to five different cities in Europe and the Middle East. While on a break in Denmark, the patient experienced a sudden onset of chest pain which he described to his wife as a burning sensation. The gentleman went to an emergency room, where he was diagnosed with an eye and lung infection and placed on a 10-day course of antibiotics. Several days later, the patient sent an email to Dr. IM requesting that a physical exam be set up.

When the patient visited Dr. IM some two weeks after the ER visit in Denmark, he said he still had burning in his chest, which he described as "like you inhale fire." Dr. IM diagnosed essential hypertension, high cholesterol, vitamin D deficiency, and migraine without aura. Spirometry was normal, and Dr. IM charted an EKG that day as normal, though the printout of the scan noted "abnormal ECG." Dr. IM noted a possible infection and extended the patient's antibiotics.

Dr. IM also prescribed benazepril (the patient was off his blood pressure medications again) and Lipitor. Dr. IM ordered a coronary calcium scan and told the patient to return in four weeks. The patient did not undergo the test before leaving the country again. Three days later, Dr. IM left a message on the patient's voice mail explaining that laboratory results were worse than previous tests and that he needed to come to the office when he returns home.

Ten days later, the patient was found dead in his hotel room in Zurich. An autopsy stated the gentleman died of "acute heart failure caused by an acute coronary infarction after fresh wall hemorrhage in a preexistent high-level constriction of the descending branch of the left coronary artery."

In a telephone call between the patient's wife and Dr. IM after the death, the wife told Dr. IM that her husband had told her that Dr. IM had cleared her husband's travels. Dr. IM charted "this would not have been my usual and customary pattern," especially with a patient with hypertension, family history, and cardiac issues. The wrongful death suit against Dr. IM filed by the patient's wife and child was resolved informally without going to trial.

Can a physician be certain that a traditionally noncompliant patient will go to a specialist on a referral? No one can know for sure, but when such a referral is absent, it is the internist who will face the liability risk.

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

Your Privacy with the Cooperative of American Physicians, Inc.

The Cooperative of American Physicians, Inc. (CAP) promotes a range of products and services designed with the welfare of physicians in mind. From the professional liability coverage provided through the Mutual Protection Trust (MPT) and the CAPAssurance Risk Purchasing Group (CAPAssurance) to the range of services and products offered through CAP and its affiliates, CAP's goal is to match healthcare providers with the best products and services — all tailored to fit their needs.

Information We Collect

When you join CAP, you provide us with personal information. We collect and use that information to service your needs at CAP, MPT, and CAPAssurance. We treat this personal information as confidential, limit access to those who need it to perform their jobs, and take steps to protect our systems from unauthorized access. The personal information we collect falls into two general categories:

- Information we receive from you on the application and other forms relating to CAP enrollment and professional liability coverage through MPT and CAPAssurance – such as your first name, last name, organization, phone number, address, email and CAP identification number; and
- Information about your transactions with CAP, MPT, CAPAssurance, and CAP's affiliates, including the CAP Physicians Insurance Agency, Inc. and the Cooperative of American Physicians Insurance Company, Inc.

Reasons We Share Your Information

We want you to feel secure about the non-public personal information you give to CAP. There are several reasons we may need to share this information:

- For CAP's everyday business purposes – for example, to process your requests, maintain and service your records and accounts, administer CAP benefits, and respond to court orders or legal investigations;
- For everyday business purposes of MPT, CAPAssurance, and CAP's affiliates;
- For CAP's marketing purposes with service providers we use, including affiliated group purchasing organizations and vendors – to offer our products and services to you;

To Limit the Sharing of Your Information

All CAP members and participants have the opportunity to tell us they do not want to receive direct marketing offers from CAP's own affiliates or other affiliated service providers. You may choose not to receive marketing offers by any method, be it direct mail, email, or fax.

To tell us your preference, you may:

Write us at:

CAP Membership Services
333 S. Hope Street, 8th Floor
Los Angeles, California 90071

Call us at: 800-252-7706

Email us at: ms@CAPphysicians.com

Fax us at: 213-473-8773

In order to ensure that we accurately fulfill your request, please provide your full name and street address, member number, telephone number, fax number for fax requests, and email address for email requests. Even if you elect not to receive product information by direct mail, fax, or email, you will continue to:

- Be contacted as necessary for routine CAP services
- Receive marketing information through our regular monthly *CAPsules* publication
- Receive notices regarding political activities affecting the medical professional liability industry and solicitations for contributions to CAP's political action committees

Of course, if you wish to continue receiving valuable and convenient product and service offers, no action is required.

December 2017

COOPERATIVE OF
AMERICAN PHYSICIANS

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

December 2017

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.
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.