

OMIC DIGEST

Ophthalmic Risk Management Digest

The Risks and Benefits of Electronic Health Records

By Hans Bruhn, MHS
OMIC Senior Risk Management Specialist

As the use of Electronic Health Record (EHR) systems continues to rise,¹ so do concerns about how their use may affect patient safety and medical professional liability. In many respects, EHR systems significantly expand upon the narrow scope of Electronic Medical Record (EMR) systems, which replace traditional paper medical records with electronic documentation tools. Because of their limited scope, EMRs have been used almost exclusively by health care providers, third party insurance payors, and government entities.

In contrast, an EHR system offers comprehensive assistance to a practice, going far beyond the scope of medical record functionality to include practice management (administration), reporting (for internal use and to external parties), coding (for billing/patient care reimbursement), and document imaging.

Additionally, an EHR system also facilitates communication with pharmacies, transcription services, surgical facilities, labs, and other external parties involved in patient care. One of the most promising functionalities that directly relates to improving patient care is the evidence-based decision support system for clinicians. From drug alerts to diagnosis assistance, EHRs offer real-time help in developing patient treatment plans.

EHR systems also provide various avenues for communicating with patients, such as messaging and allowing patient access to general e-health information and personal health information via desktop computers, PDAs, or computer tablets.²

As with any new technology, professional liability risks are emerging as EHRs are adopted on a large scale. Based on early reports, it is expected that liability claims will revolve around issues related to security and confidentiality, documentation, system integration, reporting, and data recovery. One source of these reports, EHRevent.org, is a national reporting database that represents a cooperative effort by professional liability insurers and the not-for-profit iHealth Alliance. Several of the patient care scenarios described in this article come from this source.

continued on page 4

MESSAGE FROM THE CHAIRMAN



After graduating from college, and completing 18 months of training, I began flying as an Air Force pilot with a fighter squadron in Minot, North Dakota. Professional military pilots have a demanding job. They are tasked to fly in terrible weather, over inhospitable terrain, maneuvering their aircraft at high speed, in close proximity to other aircraft approaching at high closure rates. One feels very alone in a single engine, high performance fighter 35,000 feet above the frozen tundra where the surface temperature is 45 degrees below zero. Although I recall many times feeling exposed and vulnerable, I never feared for my life because I was confident in the training I had received, the procedures and regulations established by the Air Force, the life support equipment I carried with me, and the airmen in my squadron who maintained my aircraft. I felt protected by those supporting me even as I worked in a high risk environment where inattentiveness would result in loss of life, possibly mine. Looking back 40 years later, I realize I felt safe because a "culture of safety" prevailed in my unit. It was promulgated by my commanding officer, promoted by senior staff, and followed by the 450 men and woman in the squadron.

continued on page 2

IN THIS ISSUE

- 2 Eye on OMIC**
You've Been Yelped
New OMIC Course on CD-ROM
- 3 Policy Issues**
OMIC's e-MD™ Coverage
- 6 Closed Claim Study**
Documentation Errors Related to Electronic Health Records
- 7 Risk Management Hotline**
Access to an EHR System While On-Call
- 8 Calendar of Events**
Upcoming Seminars and Courses



Eye on OMIC

OMIC

The Ophthalmic Risk Management Digest is published quarterly by the Ophthalmic Mutual Insurance Company, a Risk Retention Group sponsored by the American Academy of Ophthalmology, for OMIC insureds and others affiliated with OMIC.

OMIC, not the Academy, is solely responsible for all insurance and business decisions, including coverage, underwriting, claims, and defense decisions.

OMIC owns the copyright for all material published in the OMIC Digest (except as otherwise indicated). Contact OMIC for permission to distribute or republish any Digest articles or information. The general information on medical and legal issues that OMIC provides in the Digest is intended for educational purposes only and should not be relied upon as a source for legal advice. OMIC will not be liable for damages arising out of the use of or reliance on information published in the Digest.

OMIC
655 Beach Street
San Francisco, CA
94109-1336

PO Box 880610
San Francisco, CA
94188-0610

Phone: (800) 562-6642
Fax: (415) 771-7087
Email: omic@omic.com
Web: www.omic.com

Timothy J. Padovese
Editor-in-Chief

Paul Weber, JD, ARM
Executive Editor

Anne Menke, RN, PhD
Managing Editor

Kimberly Wynkoop, JD
Associate Editor

Hans Bruhn, MHS
Contributing Editor

Ryan Bucsi
Contributing Editor

Robert Widi
Contributing Editor

Linda Radigan
Production Manager

Photos by Mike Shore

You've Been Yelped: What You Should Know about Responding to Negative Online Reviews

The online review sites Healthgrades, Yelp, and Vitals have become a popular way for patients to research and choose an ophthalmologist. Like it or not, these (and other review) sites have virtually taken the place of the telephone book as the primary vehicle for people finding you. They also can pose a serious public relations risk for your practice since anyone can post practically anything they want—good or bad—about you in seconds, and often anonymously.

In recent months, OMIC policyholders have reported negative comments posted by both patients and disgruntled employees. Complaints have ranged from personal attacks on physicians and staff to angry and snide comments from patients who were refused drug refills or denied approval for false claims of workers compensation or disability benefits.

For more information, including tips on “do it yourself” online reputation management and recommendations on how to respond to

negative or “faked” reviews, inaccurate information, and other online threats, read the full article “You’ve Been Yelped” on OMIC’s Blog page (www.omic.com/blog—March 18 entry).

New OMIC Course on CD-ROM

Every year, 7.4% of all physicians incur a malpractice claim. By age 65, 75% of physicians who practice in a relatively low risk specialty such as ophthalmology will have been involved in at least one malpractice claim during their career, according to the *New England Journal of Medicine* (August 2011). A new audio-course from OMIC, *How to Survive Malpractice Litigation: Lessons Learned*, will explore the personal, professional, and legal issues that arise in malpractice litigation. Specifically, the faculty will discuss the importance of positive collaboration between the insured, the defense attorney, and OMIC, and how this essential teamwork helps minimize the stress of litigation and increase the potential for a favorable outcome. Upon completion of the course, OMIC insureds will receive a risk management premium discount. Contact Linda Nakamura at lnakamura@omic.com or (800) 562-6642, ext. 652, for additional information.

Message from the Chairman

continued from page 1

I have come to appreciate that hospitals, and especially operating rooms, are dangerous places too—not for the surgeon and surgical team but for the patient. Surgeons, like pilots, operate in a high risk environment where a “culture of safety” can save lives and avoid complications. What is a “culture of safety” as applied to medicine? It is a commitment to establish a safe environment for patients and to always put patient safety first. Most surgeons acquire their attitude toward patient safety early in their training. Properly taught, patient safety will remain a goal throughout their career. A “culture of safety” does not evolve from written protocols, rules, and regulations; it uses them as the means to achieve the goal. The culture is established by the decisions and actions of senior surgeons in a practice and by department chairs and teachers who themselves accept and promote the concept and demonstrate by example their commitment to patient safety.

Everyone in an organization must adopt the mantra that safe patient care is the primary measure of the organization’s success.

During the years I have been a member of the OMIC team, I have observed the board and staff’s commitment to helping insured physicians bring a “culture of safety” to the practice setting through OMIC’s underwriting guidelines, risk management courses, and confidential *Hotline*, where staff field questions and assist surgeons in dealing with patient safety issues. Refractive surgery requirements that seemed restrictive at first but which are now accepted widely and used daily; collaborative efforts with hospitals, physicians, and neonatal units to establish a safety net for infants at risk for ROP; and protocols for the off-label use of Avastin developed with the American Academy of Ophthalmology are but a few examples of OMIC’s efforts to help physicians provide a safe practice setting for patients and establish a “culture of safety” in their offices, clinics, surgery centers, and hospitals.

John W. Shore, MD
Chairman of the Board



OMIC's e-MD™ Coverage

By Kimberly Wynkoop
OMIC Legal Counsel

New liabilities are a concern when technology changes the practice environment. Now that electronic health records are becoming more prevalent, the risks they engender are also increasing. Aside from professional liability issues, health records stored electronically are at risk of hacking, unwanted dissemination, and corruption. This can be the fault of the physician maintaining the electronic health records or of an outsider. Additionally, privacy is always a concern when personal and confidential records are maintained, whether in paper or electronic form. If medical records are computerized and security is breached, privacy violations may follow.

In response to these risks, OMIC added a new additional benefit to its professional and limited office premises liability insurance policy: e-MD™ Network Security & Privacy Coverage and Data Recovery Costs Coverage. OMIC also enhanced its Patient Notification and Credit Monitoring Costs Coverage as part of the e-MD™ program.

The e-MD™ coverage provides that OMIC will pay loss and legal expenses for claims against insureds alleging network security or privacy wrongful acts. In order to understand this coverage, it is helpful to define network security wrongful acts and privacy wrongful acts. A network security wrongful act is an act, error, or omission by an insured (including an unauthorized act by an insured's employee) which results in an unauthorized use of the insured's computer system that negatively affects others. Such consequences could be the failure to prevent tampering with a third party's computer systems; the failure to prevent identity theft or credit/debit card fraud; or the inadvertent transmission of harmful or corrupt software code.

A privacy wrongful act is either of the following committed by an insured: violation of an individual's privacy rights or violation of U.S. federal, state, or local laws associated with the control and use of personally identifiable financial or medical information (e.g., HIPAA, HITECH, and Gramm-Leach-Bliley Acts).

OMIC also provides coverage for HIPAA proceedings under the separate Broad Regulatory Protection additional benefit of the policy. Under this benefit, OMIC will reimburse the insured for legal expenses incurred as a result of a proceeding instituted against the insured by a government entity alleging violation of the Health Insurance Portability and Accountability Act (HIPAA) privacy and security regulations and fines or penalties imposed against the insured as a result of such HIPAA proceeding.

Coverage for HIPAA proceedings or privacy wrongful acts arising out of the same events is afforded under either the Broad Regulatory Protection or e-MD™ additional benefit, not both, and only one limit applies. OMIC has the sole discretion to determine which coverage provision applies.

OMIC's updated patient notification and credit monitoring costs benefit provided under the e-MD™ program covers costs incurred as a result of a privacy wrongful act, but only if such costs are incurred with OMIC's prior written consent. Patient notification and credit monitoring costs include all reasonable and necessary expenses incurred by an insured in notifying patients of any actual or potential privacy wrongful act. These costs could include legal expenses, computer forensic and investigation fees, public relations expenses, postage expenses, related advertising expenses, and the costs of credit monitoring services provided to affected individuals for a period of up to twelve months.

Lastly, the e-MD™ additional benefit provides that OMIC will pay the data recovery costs incurred as a result of a data interference act, but only if such costs are incurred with

OMIC's prior written consent (unless the circumstances are such that there is no opportunity to obtain OMIC's prior written consent before incurring costs to mitigate potential damages or harm to the insured or third parties). For purposes of the additional benefit, data means any and all information stored, recorded, appearing, or present in or on the insured's computer systems, electronic communication systems, devices, and telephony. A data interference act is any act by a party other than an insured carried out without an insured's consent or knowledge that causes harm or damage to the data maintained by an insured. Data recovery costs are all reasonable and necessary sums incurred by an insured to recover or replace data that is compromised, damaged, or lost by reason of a data interference act, including the cost to repair or replace any software that is affected. Data recovery costs do not cover repairing or replacing any hardware, equipment, or wiring; the income of any insured; or recovering or replacing data that was not within the care, custody, or control of the insured.

In order for coverage to apply, the network security wrongful act, privacy wrongful act, or data interference act must take place on or after the insured's retroactive date and prior to the end of the policy period.

The most OMIC will pay per insured for legal expenses, loss, patient notification and credit monitoring costs, and data recovery costs combined is \$50,000 per policy period, and this is a sublimit of the \$50,000 Broad Regulatory Protection additional benefit of the policy.

The above is a summary of coverage. For the full terms and conditions, please see Section VII. Additional Benefits B. and C. of your OMIC Professional and Limited Office Premises Liability Insurance policy. If you believe a network security or privacy wrongful act or data interference act has occurred, please notify OMIC at (800) 562-6642 ext. 661.

The Risks and Benefits of Electronic Health Records

continued from page 1



Ensure Integrity of Record Entries

In order to be confident that an EHR system's information is accurate—and an effective defense tool in the event of a liability claim—all users should have their own login name, password, and electronic signature. Some systems use the physician's name as the author of any entry in the medical record, even those made by other staff members. Without individual password access and signatures, it can be difficult, even impossible, to determine when and who made an entry in the system. This uncertainty can lead to an entire medical record being questioned for accuracy and jeopardize the defense of a claim.

Risks of Integration with Other Systems—The Need to Verify

Because information can move very quickly between an EHR and other systems, it is essential to verify its accuracy. Here is an example:

A state prison system has an e-prescribing system that captures medication orders, prints a record for the clinician, transmits the order to the pharmacy, and notifies the nurses at "med-line" what to dispense to inmates. One morning, prisoner A was prescribed a short list of blood pressure medications. The list printed correctly. A dozen other inmates were given prescriptions, which also printed correctly. Later that day, prisoner K was prescribed numerous medications, including anticonvulsants and antipsychotics. The printout looked fine. The next day, prisoner A created a disturbance in med-line when he refused to take his pills because it was "too a big a handful." The system had dispensed prisoner K's medicines to prisoner A, who was on the brink of being forced to take them when a nurse practitioner noticed the error.³

Concerns with Automation

In an effort to save time and improve the quality of documentation, many EHR systems use drop down menus and templates. The risk here is unintentionally selecting terms

that can lead to misdiagnosis and improper treatment or using letter templates that may contain incorrect or incomplete information.

A physician reporting a claim to EHRevent.org⁴ warned, "I have witnessed occasions where I have definitely selected the correct choice, but in pulling the pen away from the screen, the menu slips down to the next selection: 'qd' can easily slip/scroll to 'qid,' resulting in a fourfold dosing error...Local pharmacists seem to be adept at catching errors and calling me, but one should not assume that will always be the case."

Overuse of templates that offer set verbiage describing examination findings and diagnoses has led some physicians to comment that it can be more difficult to review a record on a referral due to unnecessary template wording that conveys very little or no specifics of the patient's condition. A physician reporting to EHRevent.org commented, "Our EHR generates notes after you check little boxes on millions of pages of menus. The boxes are tiny and menus are incredibly detailed, so it takes forever to find what you want, and easy to miss something or check something wrong...the finished note is incredibly boring and fake, just line after line of mostly normal findings. I can't find the 'meat' in my partners' notes. My eyes actually blur. I tell myself to read every word, but all notes are 95% identical...You can't tell what actually happened at the visit, because all the notes look the same..."⁵

Plaintiff attorneys have argued that the presence of identical wording in multiple patient files is evidence that the provider did not make any real effort to document a specific patient's care, thereby attacking the integrity of the medical record and eroding defensibility of the claim.

System Reports—Verify Information and Format

EHR reporting systems need to be carefully tested and continually reviewed for completeness and

accuracy. These reports can be very different in appearance when compared to data viewed on data entry screens. Some reports pull information from various areas of the system making it harder to detect errors. As a risk management strategy, OMIC recommends carefully working with your EHR vendor to verify that reporting requirements for your practice are being met and, once your system is adopted, performing ongoing reviews of reports before releasing them to others. Duplicate entries and omitted data (requiring manual input and the potential for human error) can lead to inaccurate billing practices and upset patients.

Data Recovery—How Would You Practice Without Your EHR?

In the past few years, natural disasters in parts of the country have underscored the need for disaster planning to recover data. An insured recently contacted OMIC to seek advice on how to reestablish his practice after all his medical records, including backups, were destroyed. He did not even have a complete list of his patients due to the scope of the disaster in his area. You can avoid this extreme situation by developing a data recovery plan that truly contemplates worst case scenarios. Consider data backup in a location outside your practice area.

Even seemingly routine maintenance on an EHR system can disrupt patient care. A physician reported to EHRevent.org, "Our vendor upgrades our EHR software every 2 to 3 years. We're on an ASP (Application Service Provider in which the system is hosted on the web). We knew the system wouldn't be available intermittently over 'a day or so.' We printed out charts for the patients that had appointments. But we were down for a week! Lots of technical glitches and errors, rebooting, telephone calls back and forth. We got 'data not backed up' warnings. Temporary paper notes piled up because we couldn't do data



entry. No access to records for 90 patients we saw that week. Major staff stress.”⁶

Physicians should develop policies and procedures for periods when the EHR system is down that allows patient care to continue and ensures that documentation done off system gets into the system once it is back up and running. Keep in mind that even if your EHR system is down, patients expect the same quality of care.

In addition to down time, updates to an EHR system can alter data in the system and corrupt existing records. System enhancements or wider scale modifications should be run in a test environment first to ensure they work as intended.

Clinical Decision Support Systems

Most EHR systems now incorporate Clinical Decision Support (CDS) designed to help physicians better analyze patient data. CDS also helps a practice meet “Meaningful Use” criteria required by Medicare and Medicaid EHR incentive programs. This criteria was developed to show that a practice is using a certified EHR system that improves both the *quality* of care rendered and the *efficiency* of the delivery of that care.⁷

It is important to clarify in the EHR system agreement who has liability if a critical functionality such as CDS malfunctions and results in patient harm. OMIC recommends involving an attorney in the selection and implementation of an EHR system and to review the contract between the practice and EHR vendor. The contract should clarify who is responsible for liability claims if errors such as the ones noted here occur. The vendor should accept responsibility for system issues, especially if human error is not suspected and it is the system itself that has failed to function properly.

E-discovery—More Information Means More Scrutiny

The EHR scrupulously tracks access to records. If a provider fails to review data, such as test results that have

been received, it’s relatively easy for the patient’s attorney to discover that omission.⁸ Also, physicians should be aware that entry to the system is tracked as well as when data is entered or changed, making it easier to detect record tampering. When a correction needs to be made to the record, it is important to have a protocol and procedure in place to ensure that corrections are transparent and support continuity of patient care.

EHR Adoption Continues

Although still in the early stages, EHRs already represent a significant effort toward improving the quality and efficiency of medicine by organizing the ever increasing amount of information flowing in and out of the system, often from previously unconnected sources such as email and practice websites that allow patient interaction. So far, most practices say they are pleased with the EHR system they have adopted (73% report they are extremely satisfied or satisfied with their selected system). An increase in efficiency is not the only factor encouraging EHR implementation. Federal incentive programs are another motivator for 73% of current *non*-users who say these economic incentives will influence their decision to purchase a system.⁹

As EHR implementation becomes more widespread, the number of reported issues will grow. Through cooperative ventures with groups such as EHRevent.org, OMIC will continue to learn how such problems arise and develop risk management strategies to reduce errors. Hopefully, with a reduction in errors, the percentage of satisfied practices will grow, patient safety will be improved, and claims will be prevented.

1. 2010 AAOE member survey on EHRs reported 34% of ophthalmologists are using an EHR system.
2. Health Information and Management System Society (HIMSS) definition of EHR systems.
3. Victoroff M, MD. “I Just Eat the Skittles.” *EHRevent Report*. EHRevent.org, May 2011.
4. EHRevent.org is a claims clearinghouse set up by various professional liability carriers, the PDR Network.
5. Victoroff M, MD. “Yes—it’s a Problem: Click-tation.” *EHRevent Report*. EHRevent.org, Dec 2011.
6. Victoroff M, MD. “What Goes Up Goes Down.” *EHRevent Report*. EHRevent.org, June 2011.
7. The American Recovery and Reinvestment Act of 2009 specifies three main components of Meaningful Use: (1) the use of a certified EHR in a meaningful manner, such as e-prescribing, (2) the use of certified EHR technology for electronic exchange of health information to improve quality of health care, and (3) the use of certified EHR technology to submit clinical quality and other measures.
8. Victoroff M, MD, editor-in-chief. *EHRevent Report*.
9. 2010 AAOE member survey on EHRs.

ABOUT EHR EVENT

PDR Secure™ was established as a subsidiary of PDR Network, LLC, the publisher of the *Physicians’ Desk Reference*®, with a few simple goals in mind: to improve patient safety and to help reduce EHR vendor and health care provider liability by encouraging reporting on EHR issues. Working together with medical professional insurance carriers and the not-for-profit **iHealth Alliance**, PDR Secure has created this reporting system to gather information to help improve EHRs, support patient safety, and help reduce provider liability. By collecting and analyzing EHR-related event data reported by health care professionals, we can all get smarter together. And the privacy of information provided in the EHR Event Reporting Service can be protected by the PDR Secure™ as a certified **Patient Safety Organization**.

Report an EHR Safety Event at www.ehrevent.org/TOS.



Closed Claim Study

Documentation Errors Related to Electronic Health Records

By Ryan Bucsi, OMIC Senior Litigation Analyst

ALLEGATION

No allegations were made as these scenarios did not result in claims.

DISPOSITION

Practice revised its EHR policy to prevent a recurrence of these errors.

Case Summary 1

A technician copied a patient's medication list from the paper chart to the electronic health record (EHR). Unfortunately, the technician referenced the wrong chart so the entire list of medications was incorrect. When the error was discovered, the healthy young patient became upset that another patient's medication list had been entered into his medical record. Despite receiving a phone call and letter of apology from the administrator, the patient lost confidence in the practice and changed providers.

The group then revised its policy on medication entries to require a clinical manager to oversee and sign off on all electronic exam entries by technicians. Any errors subsequently found during audits are brought to the attention of the clinical manager and the technician at fault.

Case Summary 2

The patient's ophthalmologist was out of the office when a prescription refill request came in. An administrative assistant at the group sent the refill request to a mail order pharmacy without first getting physician approval. Unfortunately, the prescription dosage had been entered into the EHR incorrectly so the refill request was for 0.25% Timolol instead of 0.5% Timolol as the ophthalmologist had prescribed.

When the patient received the refill, she noticed the medication bottle had a blue cap instead of the yellow cap she was used to. She called the ophthalmologist to find out why the cap color had changed, which brought the medication error to the group's attention.

No harm was done to the patient and she was reimbursed for the cost of the medication. The administrative assistant, a longtime employee of the practice, was given a written warning for breach of the group's policy, which required physician sign off on all refill requests.

Case Summary 3

An ophthalmologist ordered Durezol for a patient's iritis and entered the medication into the free text area of the EHR instead of using the medication module. The scribe then sent a prescription request for Dorzolamide to the pharmacy. At a scheduled follow-up visit two days later, the technician also failed to add the prescription to the electronic medication module and copied the ophthalmologist's order from the previous visit again into the free text area of the chart for the patient's medications.

Three days after the follow-up appointment, the patient went to the emergency room complaining of increasing pain. The iritis had indeed worsened, and it was in the emergency room that the medication error was finally discovered. The patient chose not to return to the group practice after learning of the error.

A warning was issued to the ophthalmologist, scribe, and technician. The ophthalmologist was credentialed with a hospital system that required use of a different electronic prescribing system from the group's EHR. To the ophthalmologist, entering the medication in the group's EHR as well as the hospital's system seemed to be an unnecessary duplication of effort. Had she done so, however, the discrepancy most likely would have been caught and the patient would not have ended up in the emergency room.

Risk Management Principles

Electronic health records promise faster and more consistent data entry with the goal of improving patient care and safety. Redundancies are built into the system to provide opportunities to double check entries and catch discrepancies before costly mistakes are made. Still, errors do occur and inaccuracies in EHR documentation can have negative consequences for the physician-patient relationship. None of the scenarios discussed here resulted in a professional liability claim or significant harm to the patient, yet two patients chose not to return to the practice and terminated their care with the ophthalmologist.

The use of electronic health records over paper records can be a double-edged sword when claims do arise. They can either be used by the defense to support the physician's care or by the plaintiff to show a clear and undisputable record of an error.

Risk Management Hotline



Access to an EHR System While On-Call

By Anne M. Menke, RN, PhD
OMIC Risk Manager

A policyholder called today to get input on a difference of opinion in his group. The group has implemented an EHR system. One of the partners, who is an early and enthusiastic adaptor of technology, feels that ophthalmologists must access the EHR when handling after-hour calls for the group. Another physician, less technologically-inclined, is reluctant to carry a computer at all times and take on additional work if it is not necessary.

Q Am I legally required to access the EHR when speaking to a patient after-hours? Does OMIC require this?

A No. OMIC is not aware of any laws or regulations that make such access mandatory, and we have no underwriting requirements related to electronic records.

Q Do all members of the call group have to agree on whether or not to access the records?

A Patient safety studies have shown the value of a standardized approach in reducing the incidence of errors and improving communication. As in other areas of practice administration, such as appointment scheduling, prescription refills, noncompliance and billing, it is easier for staff if all physicians in a group handle issues in a similar fashion. Once the group reaches consensus, it would be helpful to develop a written protocol and train staff members in it. Policies need to be realistic and reflect goals that can be consistently reached. Such written protocols protect physicians from inadvertent criticism from their colleagues and staff if there are unexpected patient outcomes.

Q What are the risks if I don't access records?

A During telephone conversations, the health care team does not have access to the wealth of information obtained from face-to-face communication and a physical examination of the patient. Moreover, the patient may be a poor historian who does not know how to communicate what the problem is, or may not want to inconvenience the physician or appear to be whining or complaining. This situation is even more problematic after-hours, when the patient may be unknown to the ophthalmologist and medical records may not be available at the time of the telephone encounter. Making medical decisions on the basis of the limited information obtained over the telephone is, therefore, a risky—albeit necessary—aspect of ophthalmic practice. Indeed, OMIC claims experience confirms that inadequate telephone screening, improper decision-making, and lack of documentation all play a significant role in ophthalmic malpractice claims. Negligent telephone screening and treatment of postoperative patients is especially likely to result in malpractice claims. By reviewing the record, you may find information key to the diagnosis or management of the patient, such as a patient's allergy, test results, medication record, or history of recent surgeries. Without such information, you may inadvertently prescribe a contraindicated medication, or determine that urgent care is not needed. If the patient is harmed and sues, he or she may allege that failure to consult the record was negligent. As more and more physicians implement EHR systems, pressure may grow to access records after-hours, even though this care is generally not reimbursed by insurance companies.

Q What else can I do to reduce the risk of telephone care?

A First and foremost, exercise the same care when treating a patient by phone as you would during an office visit. To promote both continuity and defensibility of care: (1) gather the information necessary to assess the situation and determine the treatment plan, (2) communicate the assessment and plan to the patient, and (3) document the encounter and your decision-making process in the medical record as soon as possible after the conversation, by the next business day at least.

Q Can't I just get the information from the patient?

A You may be able to if you ask enough questions and have a patient who can reliably answer them. At other times, you may have to make a decision with limited or inaccurate information. In the absence of records, OMIC recommends using an after-hours contact log (available at www.omic.com) that prompts you to ask detailed questions about the current complaint and prior care. The form also serves to document the conversation and can be faxed to the patient's regular physician to promote continuity of care.

Q If I do access the record, how thoroughly do I need to review it?

A There is no easy answer. You face a similar situation when you take over care from another physician, or see a partner's patients in the office. The standard to which you will be held is that of a reasonably prudent physician. Obviously, you will not have time to review the entire record. At a minimum, you would want to check allergies, medication history, and recent procedures. Reading notes from the latest visits or phone calls might help you determine if the patient's condition is changing or worsening. Document which records you reviewed in order to assess the patient. To facilitate after-hours call, it would help if the record contained a front sheet with key information.



OPHTHALMIC MUTUAL
INSURANCE COMPANY
(A Risk Retention Group)

655 Beach Street
San Francisco, CA
94109-1336

PO Box 880610
San Francisco, CA
94188-0610



Calendar of Events

OMIC continues its popular risk management courses this summer. Upon completion of an OMIC online course, CD/DVD, or live seminar, OMIC insureds receive one risk management premium discount per premium year to be applied upon renewal. For most programs, a 5% risk management discount is available; however, insureds who are members of a cooperative venture society (indicated by an asterisk) may earn an *additional discount* by participating in an approved OMIC risk management activity. Courses are listed here and on the OMIC web site, www.omic.com.

Contact Linda Nakamura at (800) 562-6642, ext. 652, or lnakamura@omic.com for questions about OMIC's risk management seminars, CD/DVD recordings, or computer-based courses.

June

23 OMIC Closed Claims Studies. Virginia Society of Eye Physicians & Surgeons.* Sheraton National Hotel, Arlington, VA; afternoon session. Register at (804) 261-9890 or www.vaeyemd.org.

24 Informed Consent: Legal, Clinical, Risk Management Perspectives. Florida Society of Ophthalmology.* Ritz-Carlton Grande Lakes, Orlando, FL; 7:30–8:30 am. Register at (904) 998-0819 or www.mdeye.org.

July

1 OMIC Closed Claims Studies. Grand Canyon Regional Arizona Ophthalmological Society.* High Country Conference Center, Flagstaff, AZ; 10:45–11:45 am. Register at (602) 347-6901 or www.azeyemds.org.

27 25 Years of Ophthalmology Claims: OMIC's Experience in One State. Southeast Regional Annual Meeting for Alabama Academy of Ophthalmology,* Louisiana Ophthalmology Association,* Mississippi Eye, Ear, Nose & Throat Association,* and Tennessee Academy of Ophthalmology.* Grand Sandestin Hotel & Baytowne Conference Center, Destin, FL; 7:00 am. Register at (334) 279-9755 or www.alabamaeyedoctors.com.

29–Aug 3 OMIC Closed Claims Studies. American Eye Study Club.* Grand Del Mar Resort, San Diego, CA; time TBA. Register at www.americaneyestudyclub.org/.

August

10 OMIC Closed Claims Studies. Women in Ophthalmology.* Kingsmill Resort, Williamsburg, VA; 11:30 am–12:20 pm. Register at (414) 359-1610 or www.wionline.org.

11 OMIC Closed Claims Studies. Michigan Society of Eye Physicians and Surgeons. Grand Hotel, Mackinac Island, MI; time TBA. Register at (313) 823-1000.

September

21 Malpractice Claims Studies. North Carolina Society of Eye Physicians & Surgeons.* Grandover Resort, Greensboro, NC; 3:00–4:00 pm. Register at (919) 833-3836 or ncoph@mcmedsoc.org.

27–29 Malpractice Claims Studies. Table Rock Regional Meeting—Arkansas Ophthalmological Society,* Kansas Society of Eye Physicians & Surgeons,* Missouri Society of Eye Physicians & Surgeons,* and Oklahoma Academy of Ophthalmology.* Big Cedar Lodge, Ridgedale, MO; time TBA. Register at www.tablerockroundup.org.