An Analysis of Ophthalmology Closed Claims

By Shelly Weatherly, JD

A review of paid Ophthalmology claims from 2008-2016 revealed that inappropriate surgical technique and failure to diagnose were the most common allegations advanced. Often times the failure to timely diagnose was not the result of lack of clinical judgment or medical expertise, but rather, was the result of the failure to follow up on a test result, missed appointment or telephone message. Consistent systems and processes are part and parcel of practicing good medicine and are crucial to ensure continuity of care.

Inadequate documentation was noted to be present in 60% of the cases reviewed, and was the most prevalent factor contributing to the inability to defend against allegations of inappropriate technique or failure to diagnose. A case in point involved a 39-year-old patient who was referred to the defendant ophthalmologist with complaints of headaches, halos and eye pain. The only significant finding on physical exam was elevated intraocular pressure. The primary diagnosis was migraine with a secondary diagnosis of narrow angle glaucoma "by history". A follow-up visit was scheduled for 6 months. While the patient was instructed to return to the office if she experienced repeat symptoms prior to the follow-up visit, such was not clearly documented. One week prior to the scheduled follow-up visit, the patient called the office and requested an appointment due to a recurrence of the headaches. She denied any other symptoms so the nurse instructed her to keep the upcoming appointment but to call back if there were any new symptoms or if the headache worsened. Unfortunately, this telephone exchange was not documented. The patient did not keep the scheduled follow-up appointment. The physician would later testify that staff attempted to reach the patient to reschedule, but, again, such effort was not documented. Two years later, the patient self-referred to another ophthalmologist with complaints of increased vision loss and was diagnosed with angle closure glaucoma. The patient filed a lawsuit against the first ophthalmologist alleging failure to diagnose. The doctor argued that there were no objective findings at the time of the patient's initial presentation to support further testing, and that her failure to keep the follow-up appointment kept him from further treating her symptoms. While his medical judgment to follow the patient's condition rather than perform diagnostic testing at the time of the initial presentation may have been defensible, the patient's allegations that she called the office with continued symptoms but was denied an appointment, and the failure of any documented evidence of attempted follow-up of the missed appointment, worked against the physician.

Another example of woefully inadequate records compromising the defense of the case

involved a 62-year-old patient with a history of severe diabetic retinopathy and coronary artery disease who suffered a cardiac arrest during a retrobulbar anesthetic block. He was resuscitated but died a few days later from severe anoxic encephalopathy. The family of the patient sued, alleging that improper technique was used during the administration of the block. They alleged specifically that the physician failed to aspirate the needle to check for the possibility that such was placed in a blood vessel before administering the retrobulbar injection. They further alleged that this failure resulted in an intracranial injection of the Lidocaine with epinephrine, likely through the optic nerve sheath, which caused severe respiratory depression and cessation of breathing. Unfortunately, the procedure record was dictated 11 days after the adverse event and lacked the details needed to sufficiently defend the case. Specifically the record failed to indicate: (1) that any aspiration took place prior to the injection; (2) the amount of Lidocaine; (3) the details of the epinephrine mixture; and (4) the type of needle used. The family also alleged negligent resuscitative measures on the part of the physician and staff which was difficult to defend in light of the fact that no code record was completed to reflect interventions with the AED, compressions and oxygen.

Communication issues likewise played a part in the initiation of a number of the claims reviewed as well as the indefensibility. Problems with communication were identified in 29% of the claims reviewed, nearly all of which involved direct physician to patient communication breakdown. The failure of the physician to discuss material and significant risks associated with the procedure, as well as expected outcomes, oftentimes led to unrealistic expectations, patient frustration and dissatisfaction in the face of a complication. Further, the failure to document the process when it did occur left the door open for the plaintiffs to contend that they did not receive the relevant and required information and, if they had, would have sought more conservative treatment or a second opinion.

There were also instances of failing to properly educate patients on the specific risks associated with ocular medications to reduce inflammation, pressure and pain, and of what signs and symptoms would warrant a phone call or office visit.

LESSONS LEARNED:

- To promote continuity of care, implement a system to ensure abnormal test results are clearly flagged for follow-up at subsequent visits.
- Ensure you have an effective tracking method for all lab tests and diagnostic imaging. If a test or consult is important enough to order, it's important enough for staff to track and for providers to review results.
- There should be a consistent method for notifying patients of ALL test results and instructing them to call the office if they have not received the results within the expected time frame.
- There should be an established system for tracking patients who miss follow-up appointments. If a patient misses or cancels a follow-up appointment, it should be documented and investigated. Appropriate efforts should be made to contact the

patient and re-schedule the appointment in situations where the patient may suffer if treatment is delayed or where the treatment or medication must be closely monitored.

- Review the results of all tests ordered pre-operatively to ensure any abnormalities receive proper attention and follow-up.
- Document completely – including history, instructions and telephone calls as well as the rationale for actions that may not be self-evident. Such documentation not only enhances patient care, but bolsters your credibility if you are called upon to defend such care.
- Complete documentation within 24-48 hours of the office visit or procedure. Late completion of notes puts you and your colleagues at risk. Memory interferes with accuracy and efforts to "catch up" often lead to incomplete documentation. Any intervening adverse event prior to completion of notes makes late documentation appear self-serving.
- Develop scheduling policies and train staff that if the patient feels that his/her problem warrants an earlier appointment, the staff should communicate the patient's health problem to someone in the clinical department to triage for the best appointment option.
- Staff giving clinical advice should do so pursuant to an approved written protocol. The protocol should be detailed enough to include what clarifying questions the staff should ask in response to various complaints as well as when a patient should be referred to a physician.
- Clearly communicate with patients when providing medical advice over the telephone. Use the "teach back" method to ensure an understanding of the information relayed. At a minimum, the following types of phone calls should be documented in the medical record: All phone calls in which test results are reported to patients; all phone calls during which the patient is advised to return to the office or go to the emergency room; all phone calls during which the patient requests medical advice or prescription refills.
- Develop an emergency response protocol for the office outlining the roles and responsibilities of staff members in the event of a medical emergency. All clinical staff should maintain certification in Basic Life Support. Practices undertaking office-based surgery should be aware of any state guidelines regarding ACLS certification and/or required emergency equipment and supplies. Clinical staff should be trained in the use of any medical equipment maintained in the office. Mock drills should be conducted at least annually and assigned staff should routinely inventory medications and equipment for expiration dates and functionality. Additionally, designate the individual(s) who will be responsible for documenting the sequence of events during an emergency event.
- Engage in a full and clear discussion with patients about the nature of their medical condition, the recommended treatment plan and the risks, benefits, expected outcome, possibility of an additional or different procedure if indicated, and alternatives. Doing so not only discharges your legal and ethical obligation to provide patients with sufficient information with which to make an educated election about the course of their medical care, but may help create realistic expectations on

the part of the patient as to the outcome of treatment. Be careful not to educate above the patient's comprehension level. Be sure the details of all discussions with patients are documented in your office record rather than relying on hospital consent forms which are not procedure specific and may not capture all details of the conversation.

- Provide clear, detailed, understandable, procedure-specific written postoperative instructions to patients. Patients who have a clear understanding of what signs and symptoms to watch for, how medication should be administered and when to make follow-up appointments are less likely to be readmitted or visit the emergency department.

Although not present in the cases reviewed, national data reflects continued litigation stemming from a failure to warn of the risks of ambulating and operating a motor vehicle following the application of dilating drops. Physicians should engage is a clear discussion about the possible side effects associated with dilating drops such as blurry vision for 4 – 8 hours as well as sensitivity to light. Precautions about driving or operating machinery until the effects wear off and recommendations about protective eye gear should likewise be discussed and documented.

Importance of Effective Communication

By Jamie Wyatt, JD

"A time comes when silence is betrayal." - Martin Luther King, Jr., *The Time to Break Silence, 1967*

We are bombarded with reminders of the importance of effective communication skills in our daily lives, whether the setting is professional or personal. The importance of effective communication in the practice of medicine should never be overlooked. Effective communication needs to occur not only in the patient-physician relationship where it can have a direct effect on patient treatment as well as patient satisfaction, but also among providers where the communication of information can have life or death consequences for their patients. Lack of such effective communication also fosters opportunities for negative outcomes leading to liability exposure. Although this failure can occur either intentionally or unintentionally, both will likely result in adverse consequences. The failure to communicate information is an all-too-common factor in the difficulty of defending medical malpractice cases. Test results need to be conveyed, risks need to be addressed, confusion and/or uncertainty in orders need to be clarified, and questions need to be answered. In a surgical setting, effective communication is a must! The case below illustrates the need to speak up and communicate.

The Case

A 40-year-old male was diagnosed with an isolated atrial septal defect and underwent heart surgery utilizing bypass. Following the surgery, the patient began showing signs of right sided hemiparesis and mental changes. Tests performed after the surgery revealed strokes involving the bilateral hemispheres. Injuries included mild cognitive and physical injuries attributed to hypoxia during the surgery. The patient sued the anesthesiologist, CRNA, perfusionist, and the facility. The surgeon, who had an established relationship with the patient, was not a named party in the lawsuit. Allegations included, but were not limited to, the perfusionist's failure to keep the blood pressure within the appropriate parameters during the time the patient was on by-pass, resulting in the patient suffering bilateral strokes and neurologic injuries.

Aside from the actual treatment issues, which produced their own challenges in the defense of the case, the defensibility of the case was complicated by a number of peripheral issues. One of the most profound issues affecting defensibility involved the dynamic created by the surgeon, who was not a party to the suit. Ironically, the surgeon

imposed a practice in her operating room that inhibited effective communication. In discovery, it became clear that the surgeon had a “no talking” policy in the operating room. She prohibited anyone in the operating room from speaking except for herself. Also, due to the tense environment she created and her anger issues, the operating room staff was afraid of her. The surgeon denied a “no talk” policy during her deposition, but indicated she did not like frivolous talking. The defendants, who all testified that the surgeon would not tolerate speaking in the operating room, contradicted this testimony. Testimony from the perfusionist indicated that although she was concerned about the near-infrared spectroscopy (NIRS) monitoring values in the operating room, she did not say anything because of the surgeon’s disposition. She testified that communication with the surgeon was difficult and that she was much more comfortable with other surgeons. This deposition alone made the defense of the case challenging. Compound this testimony with the numerous co-defendant providers who all testified that the surgeon screamed at them in prior cases, intimidated them, and established a hostile environment not conducive to communication, and you have a case that adds a mad factor for any jury with the possibility of a very high jury verdict against all of the defendants.

Should the perfusionist have said something? I think we can all agree, yes! Should anyone else in the operating room have communicated any concern that they had during the procedure? Of course! And while the simple act of conveying a concern or seeking clarity of a condition could have changed the outcome of this procedure, the failure to do so resulted in significant liability among the defendants and a life changing injury to the patient. This case was settled by multiple defendants prior to trial. Clearly, the surgeon did not value the importance of effective communication nor appreciate the need to interact with the other participants in the surgery setting. The surgeon’s “no talk” policy, fear inducing conduct, and the facility administration’s failure to notice or correct the negative behavior created a hostile environment that resulted in an adverse outcome and defensibility hurdles that were impossible to overcome.

Jousting

By Julie Loomis, RN, JD

The adage about “people who live in glass houses” still holds true.

Jousting usually occurs when another healthcare professional **intentionally or unintentionally** either verbally or in the medical record makes disparaging comments about other providers, nursing staff, equipment, EHR or administration.

Often, jousting centers around comments regarding prior care, either to a patient directly or in the medical record. For example, “You mean Dr. Jones didn’t order a CT when he saw you?” Patients often have questions about another provider’s recommendations, particularly when the condition changes course and/or additional symptoms or tests reveal a different diagnosis or treatment plan. When patients are inquisitive about the care provided by another provider, simply remind the patient that you were not there and you may not have a complete understanding of the circumstances. The patient may have relayed inadequate or inaccurate information about the treatment provided, and the condition may have progressed since the time of the original care. Therefore, it would be unfair to assess another provider's judgment at the time and under different circumstances.

Jousting in the medical record, particularly if directed at a particular provider, is a gift to a plaintiff’s attorney. For example, “Dr. Smith continues to overprescribe and I’ve discussed the risks of continuing this dosage with Ms. Johnson who desires to continue the medication in spite of known risks.” Once negative comments pertaining to prior care make their way into the medical record, the defensibility of any claim regarding the care is more of a challenge. If that note ends up in litigation, it becomes evidence, and the author may also be dragged into the case, to be used as a quasi-expert to criticize the prescribing physician. Whether you have concerns about another provider or if someone is disparaging you, it is best to have an open dialogue or direct communication with that provider, rather than commenting to the patient or documenting personal opinions or comments in the medical record.

Another option is to approach a leader on the medical staff to discuss the concern. The bylaws should have a process for collegial intervention. Whatever the approach, don’t try to “defend” yourself in the medical record.

The bottom line is that plaintiffs' attorneys benefit from finger-pointing in the medical record, and healthcare professionals often take a hit to both reputation and relationships.

Commercial Payers Changing the Rules for APP Billing

By Elizabeth Woodcock, MBA, FACMPE, CPC

The reimbursement of services provided by advanced practice providers is a complex issue. Guidelines may vary based on the type of APP, and the rules surrounding APPs are impacted by federal and state regulations, facility-imposed standards of care, and billing requirements. The latter may include payer-specific protocols, which may differ by local Medicare contractor. In most cases, services provided directly by an APP (and billed as such) are reimbursed at 85 percent of the allowable physician rate.[1] When billed under a physician's identification – often referred to as "incident to," which is a Medicare term – the services are paid at 100 percent. To date, most commercial payers have followed "incident to" guidelines, allowing APPs to be billed under the physician without much ado.

Recent announcements by Blue Cross Blue Shield of Tennessee and United Healthcare have given even more complexity to this issue. If your practice employs an APP, it's important to be aware of the following promulgations by these major payers regarding requirements for billing for APPs:

- *BlueCross* [of Tennessee] *requires all nurse practitioners and physician assistants to be credentialed and contracted before providing services to its members. This includes nurse practitioners and physician assistants who are employed by a physician group already contracted with BlueCross. This requirement went into effect on Jan. 1, 2017. For more information, click here.*
- *Effective for claims with dates of service on or after September 1, 2017, United Healthcare… [is] requir[ing] physicians reporting evaluation and management (E/M) services on behalf of their employed Advanced Practice Health Care Professionals, to report the services with a modifier to denote the services were provided in collaboration with a physician. United Healthcare will accept the modifier SA on claims for these services when provided by nurse practitioners, physician assistants and clinical nurse specialists. In addition, the rendering care provider's national provider identifier (NPI) must also be documented in Field 24J on the CMS-1500 claim form or its electronic equivalent. Use of the modifier SA and documentation of the rendering care provider will assist United Healthcare in maintaining accurate data with regard to the types of practitioners providing services to its members. For more information, click here.*

These announcements signal a spotlight on payers' treatment of APPs as separate and distinct providers of care. Only time will tell if these new policies lead to better – or worse –

reimbursement rates for these practitioners.

[1] Certified nurse midwives are paid at 100% of the Medicare allowable.

New Medicare Cards with New Numbers: 3 Changes You May Need to Make

By Elizabeth Woodcock, MBA, FACMPE, CPC

The Medicare Access and CHIP Reauthorization Act of 2015 requires CMS to remove Social Security Numbers (SSNs) from all Medicare cards by April 2019. CMS will begin mailing new Medicare cards with a new Medicare number (currently called the Medicare Claim Number on cards) to your patients in April 2018. You may need to change your systems to:

1. Accept the new Medicare number (Medicare Beneficiary Identifier or MBI). Use the MBI format specifications if you currently have edits on the current Health Insurance Claim Number (HICN).

2. Identify your patients who qualify for Medicare under the Railroad Retirement Board (RRB). You will no longer be able to distinguish RRB patients by the number on the new Medicare card. You will be able to identify them by the RRB logo on their card, and we will return a message on the eligibility transaction response for a RRB patient. The message will say, “Railroad Retirement Medicare Beneficiary” in 271 Loop 2110C, Segment MSG. If you use the number only to identify your RRB patients beginning in April 2018, you must identify them differently to send Medicare claims to the RRB Specialty Medicare Administrative Contractor, Palmetto GBA.

3. Update your practice management system’s patient numbers to automatically accept the new Medicare number or MBI from the remittance advice (835) transaction. Beginning in October 2018, through the transition period, CMS will return your patient’s MBI on every electronic remittance advice for claims you submit with a valid and active HICN. It will be in the same place you currently get the “changed HICN”: 835 Loop 2100, Segment NM1 (Corrected Patient/Insured Name), Field NM109 (Identification Code).

If you use vendors to bill Medicare, contact them if they haven’t already shared their new Medicare card system changes with you; they can also tell you how they will pass the new Medicare number to you. Visit the New Medicare Card Provider webpage for the latest information.

Disgruntled or Dishonest Employees May Be the Source of a Security Breach

By

With all of the security breaches in the news recently, many medical practices have taken extra steps to keep their patient records safe. Employee training and awareness, installation of virus and malware protection, regular data back-up, purchase of a cybersecurity insurance policy, and hiring an IT person to help keep systems up to date are examples of ways to make a medical practice more secure. However, no matter what is done to protect sensitive data, sometimes the biggest threat to patient records is located right in your office.

Employees must have access to sensitive data, such as patients' protected health information (PHI) in order to perform their job duties. However, sometimes employees will access information that is outside the scope of their employment. Employee access of PHI without a job related reason could be considered a criminal violation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. In addition, this type of unauthorized access of PHI generally requires the practice to notifiy the patient, government and in some cases the local media under the Breach Notification Rule.

Many times, a breach of PHI is unintentional. A patient's PHI may be inadvertently mailed to the wrong patient, or a patient's lab results are accidentally handed to the wrong person. However, in some cases an employee may have less than honorable intentions when accessing sensitive data. In all cases, the SVMIC policyholder should report the incident as soon as it is discovered to the claims department.

The following are examples of actual claims that illustrate circumstances when an employee was the source of a breach. These claims are being responded to by NAS Insurance Services either through the coverage included in the SVMIC professional liability policy or in additional limits purchased through SVMIC's partnership with NAS:

- A practice received an anonymous call advising that a current employee was selling their patients' personal information. The caller proved this by giving the manager names, social security numbers and dates of birth of three patients.
- A long time billing employee was terminated. It was discovered that he had run several reports including patient data that were unrelated to his job duties. It is

unknown for what purpose he gathered the information. In addition, he had previously admitted to another employee that he had taken credit card receipts with account information for many patients, and two receipts were found in his desk. Fortunately, to date there have not been any complaints from patients regarding their credit card accounts.

Disgruntled or dishonest employees are often at the root of cybersecurity claims reported to NAS. In some circumstances, an unhappy employee may decide to take records with them when they leave, as in the following examples:

- Two employees left a policyholder's employment under unfavorable terms. The policyholder learned that these former employees downloaded patient information to a flash drive and took it with them when their employment ended. This claim is being covered under the cyber liability provision of the practice's SVMIC cyber coverage.

- An enterprising nurse left the employ of one plastic surgeon and went to work for a different plastic surgeon. The first practice was notified by several patients that they had received emails from the nurse advising them that she had left and inviting them to transfer their care to her new employer. This is unauthorized use of electronic data since she was no longer an employee. The practice's cyber liability policy will cover this situation.

As mentioned previously, to safeguard patient data, practices may rely on an IT expert. In order to do so, the IT expert is granted access to the entire system. However, if the relationship should ever become hostile and the trusted expert is no longer trustworthy, their access gives them the ability to destroy or otherwise keep data from being accessed by employees. For one medical practice, that is exactly what happened:

- The quality of work of the contract IT employee that the practice used for all of their computer work had deteriorated and it was time to end the employment agreement. There was a fee dispute, and in retaliation the IT employee remotely accessed the practice's computer systems and blocked the group's access to their billing and business records. The group's cyber liability coverage provided within their SVMIC policy is helping the practice recover any unavailable records.

Health and Human Services (HHS), the agency that enforces HIPAA rules, requires the practice to have protocols that outline the circumstances in which PHI can be accessed and what to do once unauthorized access is discovered. As a first step, a unique username and password for each employee who has access to sensitive data is one way to ensure that only those employees who are authorized to access patient records are able to do so. However, the responsibility of the practice does not end with a secure login. The HIPAA Security Rule requires certain administrative, physical and technical safeguards to be implemented to protect the confidentiality, integrity and availability of all electronic PHI that the practice creates, receives, transmits and stores. The following technical safeguards are outlined on the HHS website:

Technical Safeguards

- Access Control
- Audit Controls
- Integrity Controls
- Transmission Security

In addition to compliance with the HIPAA Security Rule, it is necessary that a practice have a plan in place for when a breach is discovered. For instance, there are steps to take to determine the extent of the breach. Once it is determined how many records are involved, there are rules regarding notification. These rules apply not only to a cyber-attack but also to the examples listed above. The following checklist can be found here:

In the event of a cyber-attack or similar emergency an entity:

- Must execute its response and mitigation procedures and contingency plans.
- Should report the crime to other law enforcement agencies, which may include state or local law enforcement, the Federal Bureau of Investigation (FBI), and/or the Secret Service.
- Should report all cyber threat indicators to federal and information-sharing and analysis organizations (ISAOs), including the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs.
- Must report the breach to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals, and notify affected individuals and the media unless a law enforcement official has requested a delay in the reporting.

For more information regarding these security and response requirements, visit https://www.hhs.gov or https://www.healthit.gov. For additional information regarding the Breach Notification Rule and the steps that must be taken when a breach occurs, visit https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

Overpayments

By Laura Watkins, FACMPE, CPC

When was the last time your credit balance report was reviewed and worked thoroughly? Working the report on a regular basis is an essential step in the revenue cycle.

Understandably, many practices focus on the collection of insurance and patient payments portion of the revenue cycle. Overpayments are often the last priority. However, medical practices can face considerable compliance exposure when it comes to overpayments, especially with Medicare.

In February 2016, the Centers for Medicare and Medicaid Services (CMS) published its final rule addressing a requirement in the Affordable Care Act relating to Medicare Part A and Part B providers and suppliers. The Rule, effective March 14, 2016, includes a provision that providers report and return an overpayment, regardless of the cause, within 60 days after the date it identifies the overpayment for government programs. An overpayment is considered funds received and kept under the Medicare programs to which the practice is not entitled. CMS published the Final Rule that offered some clarity about when the 60-day rule started. “The 60-day time period begins when either the reasonable diligence is completed or on the day the person received credible information of a potential overpayment if the person failed to conduct reasonable diligence and the person in fact received an overpayment.” 81 Fed. Reg at 7661 (“Rule”).

Reasonable diligence would consist of both proactive compliance activities of a possible overpayment and reactive investigations. CMS expects providers to participate in proactive compliance actions, such as random audits, that assist in the identification of potential overpayments. When a provider receives credible information about a possible overpayment then he or she must perform a reasonable inquiry to determine if an overpayment exists and quantify the overpayment amount. The provider has 6 months after receiving the information to respond to the inquiry; and if it is determined that an overpayment did occur, the provider has 60 days to report and return the overpayment.

If a provider fails to comply, he/she could potentially face False Claims Act liability, civil monetary penalties and exclusion from federal healthcare programs. In addition, providers can expect increased enforcement of this provision by the government or whistleblowers.

When analyzing a practice’s revenue cycle, our medical practice consultants often find that physicians and managers do not proactively research credit balances and issue refunds in a timely manner. The Final Rule focuses on Medicare overpayments; however, it is important to work all overpayments. Ignoring credit balances can also have an effect on your total accounts receivable (AR). Depending on how a practice filters their AR report,

your balances may be distorted. If accounts with credit balances are included in the AR report, your balances will be offset by the credits causing the overall AR balance to be less than it actually is. The benchmark for credit balances should be less than two percent of your total AR.

What if a refund cannot be returned because a patient has moved and left no forwarding address? Each state has an escheat law that directs how your practice should handle refunds to the payers or patients.

Failure to comply with the timely investigation of overpayments exposes the practice to considerable risk. If your practice does not have an established routine for auditing for overpayments, this should move to the top of your "To Do" list. The fines associated with the False Claims Act are three times the amount of the false claims plus civil penalties of $10,957 to $21,916 per false claim.
