MACRA 2.0 Proposed

By Elizabeth Woodcock, MBA, FACMPE, CPC

Proposed updates to the Medicare Quality Payment Program (QPP) for calendar year 2018 would provide many physicians and other providers welcome relief from several regulatory burdens imposed by the Medicare Access to Care and CHIP Reauthorization Act (MACRA). The updates also would give tens of thousands clinicians new avenues to opt out of the program altogether without penalty.

Most notably, the proposed rule, released June 20, 2017, by the Centers for Medicare & Medicaid Services (CMS), would expand MACRA hardship exemption options and raise the thresholds for mandatory participation — both steps lowering the number of clinicians required to participate in certain MACRA programs.

The rule would raise the mandatory QPP participation threshold – measured in total allowed Part B charges – from $30,000 to $90,000 during the reporting period. Those receiving less than $90,000 in total allowed Part B charges would not have to participate. Similarly, those seeing fewer than 200 Medicare patients during a reporting period could opt out of the QPP. CMS estimates that this proposal alone would excuse some 30 percent of practicing physicians from participating in QPP — that's in addition to the 35 percent who are already exempt. For the estimated 35 percent of the nation's clinicians who would remain eligible for the QPP, the CMS proposed rule offers options to relieve several of the program's most onerous requirements.

One major area of relief applies to small practices, which CMS defines as 15 clinicians or fewer. Those in small practices who still met the new participation thresholds – more than $90,000 in Part B total allowed charges or more than 200 Medicare patients during the reporting period – could declare a hardship exemption for the Advancing Care Information (ACI) category, formerly known as Meaningful Use. Physicians practicing in a rural area or that which is designated as a Health Professional Shortage Area (HPSA) also could opt out of ACI under the newly proposed hardship exemption.

The rule, which takes MACRA into its second year of implementation, would further delay the cost category of the Merit-Based Incentive Payment System (MIPS). Furthermore, clinicians could continue using 2014 Edition Certified Electronic Health Record Technology (CEHRT) for another year, which is especially good news for the many practices feeling pressured to purchase costly required upgrades to the 2015 version. For practices with "decertified" systems, CMS proposes an exemption in 2018 that would be retroactive to the current (2017) reporting year.

Other changes in the proposed second year of the QPP include:

- Bonus points in the MIPS quality category for small practices submitting data on at least one performance category, plus individual bonus points to providers whose patient populations are considered complex as defined by their average Hierarchical Conditions Category;
- New MIPS reporting option giving hospital-based physicians greater flexibility in reporting (they would be able to use their facility's inpatient value-based scores to calculate their individual scores in cost and quality if they wished);
- MIPS participation avenues for non-affiliated physicians of any specialty to band together to participate as a virtual group in the QPP;
- Use of multiple submission mechanisms even if they were within the same category (for example, measures for the quality category of the QPP could be transmitted via an EHR *and* via a registry); and
- Addition of exclusions for the summary of care record exchanges and e-prescribing in the ACI category.

The rule still takes steps to move MIPS forward; for example, clinicians would have to submit 12 months or more of data to earn sufficient points in the quality category and avoid penalties. The proposal also continues the three-point floor for each quality measure, with the exception of those that do not meet the data completeness requirements and are not a small practice. It also accords a maximum of only six points for those measures that are "topped out" (compared with a potential of 10 points that can be earned for all other measures).

While the theme of the 2018 proposed rule is clearly "relief," there are many recommended changes in the 1,058-page proposal. For those physicians who remain eligible, familiarity with what is still a tangled web of rules must be a priority for success in the years ahead.

It Adds Up Quickly

By Kari Stearn

Over the past decade, rapid advancements in technology have enabled a vast and expansive digital economy. As a result, medical practices of all sizes are using a broad range of personal and company-issued devices to keep employees connected to each other and to their workplace. But as connectivity grows, so too does the number of cybersecurity risks and threats.

It has been shown time and again that a seemingly harmless act like a misplaced laptop or a casual click in an email can put a practice, its employees, and its patients at risk. While we're constantly innovating to keep pace with these risks, we believe that education and preparedness is equally important when it comes to mitigating and preventing a cyber breach.

The claim below provides a real-life example of the impact and costs of a cyber breach, and the protections provided by cyber insurance.

An employee of a medical research institute carried his laptop with him to and from work each day. One day, the employee left the laptop in his car and returned to find the laptop had been stolen. The employee informed the institute, and the institute immediately notified its cyber insurance carrier of the incident. The carrier engaged legal counsel and an IT/forensics vendor to investigate the nature and scope of the data stored on the laptop. The findings revealed that the laptop contained the electronic protected health information (ePHI) of approximately 296,000 patients and research participants, including names, dates of birth, addresses, social security numbers, diagnoses, and laboratory results.

Because of the sensitive nature of the information stored on the laptop and the fact that the laptop was only password-protected and not encrypted, the institute was required by law to notify all affected individuals. As required by federal law, the breach was also reported to the Department of Health and Human Services, Office for Civil Rights (OCR), who launched an investigation. In addition, a public relations firm was hired to handle media inquiries and communications.

The OCR investigation revealed a host of violations and inefficiencies on the part of the institute. The agency determined that the institute's security management process violated HIPAA law because it was limited in scope, incomplete, and insufficient to address potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the institute. Further, the OCR claimed that the institute had failed to implement

proper mechanisms to safeguard ePHI and lacked appropriate policies and procedures for authorizing access to ePHI. To make matters worse, the institute faced multiple lawsuits filed by individuals affected by the breach.

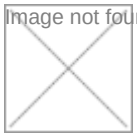
Costs associated with the breach escalated quickly. Privacy breach response costs amounted to $960,000, including IT/forensic expenses, public relations fees, legal expenses, notification costs and credit monitoring. Defense expenses incurred in the OCR proceedings and patient lawsuits reached $860,000, and settlements amounted to a combined $2.1 Million. While the institute's cyber incident costs totaled $3.92 Million, $2.82 Million was covered by the policy, and the institute was responsible for the remaining $1.1 Million.

As previously announced, SVMIC added Cybersecurity Insurance as a supplemental coverage to each physician's policy and each practice entity's policy a couple of years ago. Please note, however, that it is "basic" coverage in that the coverage limits in most cases is up to $50,000, which is enough for some cyber-related claims but certainly not for situations described above. SVMIC recommends that practices review their individual situation to assess whether their needs are covered by this basic coverage. For more information, please contact SVMIC at 800.342.2239.

An Analysis of Neurosurgery Closed Claims

By Shelly Weatherly, JD

A review of Neurosurgery closed claims from 2004 – 2016, where a loss was paid on behalf of an insured, reveals that there were 3 basic areas (excluding errors in medical judgment and/or technical performance) that contributed to the indefensibility of the claims. These topics are illustrated in the graph below:



DOCUMENTATION ISSUES: Documentation is one of the most important patient care and risk management skills a healthcare professional can develop. Inadequate documentation can negatively impact your ability to defend the care provided to a patient.

As the graph above illustrates, documentation issues were a factor in 60% of claims paid in neurosurgery. Of those, 57% involved inadequate documentation due to such things as:

- incomplete pre-op work-up and patient history
- incomplete or no documentation of patient phone calls
- lack of sufficient information to support rationale for treatment decisions
- sparse or lacking documentation of information given during the informed consent process
- non-specific or incomplete discharge instructions.

A specific case example involved a patient who presented to the ED with complaints of neck pain the day after fainting and falling at her home. A CT and X-rays of the cervical spine were ordered which revealed a C5-C6 fracture. The patient was admitted and a neurosurgeon was consulted who ordered a MRI which, in addition to the fracture, revealed a moderate sized epidural hematoma beneath the C5 and C6 lamina. The patient was discharged the next day since her pain level had improved, she was neurologically intact, was ambulating, had full strength and had no complaints of radiating pain, numbness or tingling. The written discharge instruction advised the patient to wear a neck collar at all times and to follow up with the neurosurgeon in 6 weeks. Although the neurosurgeon would later testify he also instructed the patient to return to the ED immediately should she experience worsening pain, numbness or weakness, he did not document such in the discharge instructions. The patient returned 2 days later with complaints of weakness in her right leg and hand and having a “funny feeling.” An MRI revealed a significantly larger hematoma that was compressing the cord. The hematoma

was evacuated, but the patient was left with permanent neurological deficit following a lengthy course of rehabilitation. The patient filed suit, alleging failure to timely perform surgery to evacuate the hematoma and failure to provide specific discharge information. While the neurosurgeon's decision to discharge the patient following her initial presentation was defensible given the apparent stability of the fracture, the lack of documentation as to his specific instructions and warnings that would warrant an immediate return to the ED created a swearing match and hampered the defense of the case.

Untimely entries were also a problem in several cases reviewed. Operative notes and discharge summaries dictated weeks, and on occasion, months after the fact often appear self-serving and call into question the integrity of the entire record.

SYSTEMS ISSUES: Effective systems and processes serve to reduce human error that may lead to patient harm. In the cases reviewed, 35% included a systems breakdown, the majority of which (55%), involved wrong site surgery. Examples of factors that led to wrong-site procedures include:

- Reliance on improper site verification by the patient
- Entry of the wrong level into surgeon's mobile device
- Failure to refer to intraoperative studies which contradicted erroneous documentation of the operative site contained in the Consent and Pre-Op Verification forms
- Reliance on a substandard location x-ray
- Failure to confirm the correct level radiographically

Often times, the initial error was compounded by the failure of the surgeon to timely review post-op studies which would have led to earlier recognition and corrective surgery. However, when the wrong site was discovered either intraoperatively or immediately postop, and patients were advised of the error forthrightly and promptly, settlement amounts were typically reasonable.

Other systems errors involved retained foreign objects. One case involved a 61-year-old patient who underwent a decompressive laminectomy. Following the procedure, the sponge count was incorrect so the surgeon ordered a lateral x-ray that he read as negative for retained objects, which led to the conclusion that the nurse had miscounted. Subsequently, the film was over-read by a radiologist who observed the sponge. The radiologist's report was filed in the surgeon's office without his review. The patient presented to the office several times over the next few months complaining of pain but the surgeon did not refer to the report in his file. Finally, at one of the visits, the physician noticed a palpable mass on the lower spine and a repeat lumbar spine film revealed the sponge.

Failure to follow up on abnormal test results was likewise a recurrent theme in the cases reviewed. The typical situation is illustrated by the case involving a patient who was discharged post operatively without any action being taken on abnormal results from an

intra operative culture. He developed a spinal abscess requiring surgery. In another case, a patient was admitted with head trauma. An MRI revealed a possible berry aneurysm and the radiologist suggested angiography. The surgeon did not see the report. The surgeon's LPN dictated the discharge summary but failed to include the MRI findings. Six weeks later, EMS transported the patient to the hospital in critical condition with a ruptured aneurysm.

COMMUNICATION ISSUES: Effective communication is essential in establishing trust and building good patient rapport, which in turn leads to better patient compliance. Of the cases reviewed, 32% involved communication breakdowns. Of those, 75% involved a breakdown in communication between the physician and patient. Common examples include:

- Insufficient patient counseling: Failure to educate regarding the impact of smoking on surgical healing
- Inadequate discharge instructions: Failure to instruct as to what post-op symptoms to look for and when to notify the physician
- Lack of informed consent: Failure to review pertinent risks, benefits and alternatives to the proposed procedure, and to ensure patient's questions are answered

LESSONS LEARNED:

- Document timely and completely - including history, pre-op workup, instructions, telephone calls, the rationale for actions that may not be self-evident and post-op instructions and warnings. Be very clear about which symptoms require immediate physician notification or follow-up care at an emergency department.
- Engage in a full and clear discussion with patients about the nature of their medical condition, the recommended treatment plan and the risks, benefits 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 patient's part as to the outcome of treatment. Be careful not to educate above a 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 that are not procedure specific and may not capture all details of the conversation.
- Provide procedure-specific written postoperative instructions to decrease the possibility of non-compliance and reduce the number of callbacks from patients and family who may not remember your verbal instructions.
- Use the Universal Protocol designed to prevent wrong patient/site/procedure surgeries by marking the surgical site appropriately with the patient/representative prior to surgery and use a time out to review relevant aspects of the procedure with the surgical team and to ensure verification and reconciliation of patient information prior to starting the surgical procedure.
- Have all available films and studies that support the planned procedure on hand in the OR.
- When encountering an inaccurate sponge/instrument count, thoroughly review the x-

rays and seek radiology assistance if needed.

- Make it your policy to follow-up on all radiology over-reads.
- Have a mechanism in place that prevents labs and radiology reports from being filed or scanned into the EMR prior to your review and sign off.
- In the event of a medical error, have a frank discussion with the patient and family including a description of the events, without either accepting or placing blame, along with a sincere acknowledgment of regret for the unfortunate nature of the event. Call an SVMIC Claims Attorney to discuss – 800.342.2239.
- The operating surgeon is responsible for the content of the discharge summary. It is important to be aware of state and hospital rules, regulations or opinions that may prohibit delegating this duty.

The New Reality of Patient Financial Responsibility

By Elizabeth Woodcock, MBA, FACMPE, CPC

As insurers and employers are now offering health plans with higher deductibles and copayments, collecting at the point of contact is more important than ever to ensure a successful practice. While many medical practices struggle with this, it doesn't need to be as difficult or intimidating as it might first seem. In fact, point-of-service collections can bolster your practice's profits amidst the growth of consumer-driven health plans.

The challenge, of course, is that many insured patients don't examine their health plans in detail, focusing instead on payments of premiums and provider networks, if anything. Patients rarely take a close look at the totality of financial responsibility, and are often surprised by medical bills. If the percentage of financial responsibility remained low, this consumer ignorance wouldn't have an impact on medical practices. However, insurers are shifting an ever-increasing percentage of financial responsibility to patients.

Despite this trend, many practices collect only a fraction – if any – of what patients owe at the point of service. They hope to receive the rest in time, but then must deal with printing and mailing costs, accounts receivable management and, eventually, collections. As the reimbursement landscape continues to shift along with the patient's responsibility, this model is not tenable for the long term.

Collecting at the point-of-service is undoubtedly a sensitive topic, but it can no longer be ignored. The following tips will help your medical practice be successful in this new reality.

Get employees involved. Train staff on how to collect money. Ensure that employees know where to look in the system for the patient's financial responsibility, both current and past. In addition to today's responsibility, request that employees ask for all balances. Inquire about balances during the scheduling process, in addition to the patient's arrival at the front office. Change the way you ask patients for payment from "will you be making your copayment today?" to "will you be paying by cash, check or credit card?"

Measure the performance of employees by monitoring collection activity, by staff member. Hire the right employees in the first place, with skills related to collecting money, particularly for your front office positions.

Offer the right signage. Instead of a post that reads, "As a patient of our practice, you must pay your copayment at time of service," print signs that state, "Your health plan requires

payment of your copayment at the time of service." This subtle change shifts responsibility from your practice to the health plan – accurately - and makes this request easier for employees.

Determine what to collect. Your practice may decide to just stick with copayments, but it pays to revisit your protocols for point-of-service collections. Estimate what you should collect at point of service – from copayments to balances, and perhaps even unmet deductibles, pre-service deposits, and fees for non-covered services. While this entails some effort, determining each patient's financial responsibility will simplify and streamline the process for employees.

Offer the support and answers patients need. Answer questions calmly and patiently, without exhibiting frustration or disdain. Provide employees at the front office training in basic concepts like deductibles, as well as access to the details of patients' coverage and benefits eligibility. Consider offering read-only access to explanation of benefits, thus allowing employees to reference the details related to the balance for an insured patient, and perhaps even sharing access to the screen in order to better the patient's understanding.

Train to handle a refusal of payment. Despite best efforts, there will be times where a patient refuses to pay. Take the opportunity to determine your practice's protocols in this scenario: will the payment request be emphasized one last time after checking in the patient or will care be refused? While the temptation may be to turn the patient away for failure to pay, it is important to understand the risks associated with this protocol. Confer with the physicians in developing processes within your practice surrounding refusal of care based upon ability to pay.

There is no time like the present. While it might be tempting to tell a patient to contact their insurer and get back to you, it is best to get matters resolved as they are happening. Give your patients the option to use an in-house phone to make a call or ask your billing manager to talk with the patient in a private area, if needed.

If employees are unable to collect at the point of service, ask them to make a record of it. Note the date, amount owed and the reason payment was not collected. This documentation is vital for successful post-visit collections, as well as providing information to improve future training efforts. These records will also give you the opportunity to pinpoint patterns by patient, procedure, physician, employee, day of the week and so on. Simply requiring the documentation of this information can increase employees' compliance with your protocols.

Granted, collecting money is not anyone's favorite part of the job, but the act of collecting on time, every time will ensure your practice continues to serve your community for many years to come.

"We Are Sorry to Have to Inform You"

All seemed well at a busy pediatric practice until a routine audit conducted by the Vaccine for Children program (VFC). When the VFC auditor reviewed the temperature log for the practice's vaccine storage unit, numerous temperatures were noted to be out of conformity with guidelines. Non-conforming temperatures had been recorded sporadically over approximately a nine month period, during which a significant number of children had received standard pediatric immunizations. VFC notified the Centers for Disease Control, and the practice promptly took appropriate remedial actions.

The practice's vaccine storage unit was a combo cooler, with a refrigerator compartment and a freezer compartment, each monitored by a temperature probe connected to a battery operated thermometer mounted on the exterior of the unit. (Each cooling compartment also had a thermometer affixed to its inner wall, but data from those devices was not routinely noted, because they indicated temperature in Centigrade, while the temperature log called for readings in Fahrenheit.) A temperature log was kept, noting a refrigerator range of 36 to 42 degrees Fahrenheit and a freezer setting of 5 degrees. Readings were to be taken twice daily but often were logged only once. During the months in question, logged temperatures were unpredictable and variable, with non-conforming refrigerator readings on some days and non-conforming freezer readings on other days, with rare overlap. The log was counter-signed by a physician, and non-conforming readings were reportedly brought to the attention of the practice administrator (soon to be ex-administrator), but other than occasional adjustments to the unit's settings, no action was taken to identify the cause of the concerning temperatures.

Following the VFC audit, the practice replaced its vaccines. It also purchased a new thermometer for the refrigerator and a separate one for the freezer. Interestingly, the new thermometers consistently indicated temperatures within guidelines, while the old thermometer continued to show non-conforming readings, indicating the likelihood that the culprit was the thermometer itself or perhaps its battery, rather than the refrigeration unit. Nonetheless, because of the many logged temperatures outside of guidelines over such a long period of time, the practice, with legal advice and in consultation with the CDC, elected to notify all patients who had received vaccines potentially rendered ineffective by storage temperatures outside of manufacturer recommendations. A "Dear Parents" letter was composed, beginning, "We are sorry to have to inform you …" and explaining the recommendation for re-vaccinations, to be provided free of charge. The re-vaccination program was completed uneventfully but at considerable cost to the pediatric practice.

Things could have been worse. In January 2017, New Jersey's Medicaid Fraud Division temporarily suspended a pediatrician and his practice from that state's Medicaid programs, based upon findings that the practice had improperly stored vaccines administered to children as part of the VFC program. The suspension was later lifted, based upon a

settlement that included modification of certain office practices and a very substantial monetary penalty.[1] An isolated incident? As to the penalties, perhaps. As to proper storage of vaccines, perhaps not. In June 2012, the Department of Health and Human Services issued a report describing “vulnerabilities in vaccine management” in 76% of the 45 VFC participating practices selected for screening. The report cited deficiencies as to storage temperatures, storage of expired vaccines with unexpired vaccines, and adequate documentation.[2] To borrow a quote from the political realm, “Nobody knew health care could be so complicated.”

Some medication safety issues are more obvious than others. This article illustrates one issue which may tend to fly beneath the radar but which can have very serious implications for patients, physicians and practices. Following are two links to CDC information and materials that may help your practice avoid the pitfalls described.

https://www.cdc.gov/vaccines/hcp/admin/storage/toolkit/storage-handling-toolkit.pdf

https://www.cdc.gov/vaccines/hcp/admin/storage/index.html

[1] Press release, Office of the State Comptroller, Medicaid Fraud Division, May 2, 2017

[2] Department of Health and Human Services, Office of Inspector General, “Vaccines for Children Program: Vulnerabilities In Vaccine Management,” June 2012

If the "Scribe" Fits

By Sheri Smith, FACMPE

Physicians struggle with the increased regulatory requirements of documenting a patient encounter in the Electronic Health Record (EHR). The majority of physicians chose medicine as a career path to take care of patients only to find that they spend an overwhelming amount of time and energy documenting patient encounters. One option that some physicians have found helpful is the use of scribes to help ease this burden. Let's take a look at some examples of the benefits practices have realized with the use of medical scribes.

A large cardiology practice uses medical scribes by having them accompany each physician into the exam room to document the patient encounter directly into the EHR as the physician verbalizes the assessment. Additionally, the scribe gathers data for the physician including nursing notes, prior records, labs and radiology results. "Our medical scribes do the bulk of the documentation for the physicians," says one of the cardiologists in this practice. "They are handling about 80% of the ancillary duties for us. It has been the best investment we have made."

A solo dermatologist uses his LPN as a scribe. This physician comments, "She does 75% of my documentation. She enters vitals, medication and recent medical history. Upon entering the exam room, I assess the patient and verbally dictate my findings as she documents directly into the EHR. I then go into the next exam room without ever touching the computer. I have more one on one with my patients and know I provide much better patient care."

Whereas some practices realize positive benefits, this is not always the case. A primary care practice tried numerous times over the course of two years to use scribes. After talking to colleagues, reading articles about the increase in productivity, the efficiency in the clinical area and the reduction of the documentation burden, using medical scribes seemed like the best thing for this busy practice. Unfortunately, for them it did not work. The physicians and staff put much effort into making this successful, but the complexity of the patients' visits, variety of complaints, and numerous procedures performed in the practice made it difficult for the scribes to keep up and document the information correctly.

With the continued push to document a more detailed patient encounter for not only liability reasons, but also for better coding, we are seeing a growth in the use of scribes. The American College of Medical Scribe Specialists estimates that physicians and hospitals will employ approximately 100,000 medical scribes by 2020. While this number continues to grow, the position remains minimally regulated. The only certification

program offered for scribes in the United States is by the American College of Clinical Information Managers (ACCIM). A significant number of medical scribes are not certified. Essentially, the physician is the one who decides the level of risk he/she is willing to accept when using a scribe.

Scribes have almost the same security rights in the EHR as the physician, while a clinical assistant enters information independently within his or her range of responsibilities. A scribe's responsibility, on the other hand, is to enter exactly what the physician says during that patient's visit. If a scribe is not properly trained or familiar with medical terminology, medications, procedures, etc., false or incorrect information can easily be entered into the EHR. To make sure there is no misunderstanding between the role of a scribe and a clinical assistant, it is essential the scribe logs into the EHR and documents as a scribe and not as a clinical assistant. The two roles are performed differently and security rights/documentation in the EHR should reflect that distinction.

A scribe is an extension of the physician, and it takes time and effort to train scribes to manage physician workflow while not exposing the provider to additional risk. The scribe job description is unique in medical practices in that they are exclusively dependent on physicians. If the decision is made to use medical scribes in your practice, take the time to establish policies and procedures regarding responsibilities, carefully manage the process/workflow, set clear goals, and monitor and conduct on- going training. Organizations such as the American Health Information Management Association (AHIMA) provide practical suggestions, which may be useful in developing policies and procedures.

Whether you decide a scribe is right for your practice or not, it is definitely a trend in healthcare right now and something to consider. With an increasing documentation burden, many practices are seeing the use of scribes as a cost effective and efficient way to help physicians spend more time with patients. Be aware that using scribes comes with risks, though, and use resources that are available to ensure you mitigate these risks to the maximum extent possible.

[1] https://theacmss.org/wp-content/uploads/2016/08/ForTheRecordAug2016.pdf

[2] http://library.ahima.org/doc?oid=106220

The Joint Commission issued guidelines in the use of scribes in healthcare organizations:[1].

The Joint Commission does not endorse nor prohibit the use of scribes. However, if your organization chooses to allow the use of scribes the surveyors will expect to see:

- Compliance with all of the Human Resources, Information Management, Leadership (contracted services standard), Rights and Responsibilities of the Individual standards and Record of Care and Provision of Care standards including but not limited to:

- A job description that recognizes the unlicensed status and clearly defines the qualifications and extent of the responsibilities (HR.01.02.01, HR.01.02.05).
- Orientation and training specific to the organization and role (HR.01.04.01, HR.01.05.03).
- Competency assessment and performance evaluations (HR.01.06.01, HR.01.07.01).
- If the scribe is employed by the physician all non-employee HR standards also apply (HR.01.02.05 EP 7, HR.01.07.01 EP 5).
- If the scribe is provided through a contract then the contract standard also applies (LD.04.03.09).
- Scribes must meet all information management, HIPAA, HITECH, confidentiality and patient rights standards as do other hospital personnel (IM.02.01.01,IM.02.01.03, IM.02.02.01, RI.01.01.01).
- Signing (including name and title), dating of all entries into the medical record-electronic or manual (RC.01.01.01and RC.01.02.01). For those organizations that use Joint Commission accreditation for deemed status purposes, the timing of entries is also required. The role and signature of the scribe must be clearly identifiable and distinguishable from that of the physician or licensed independent practitioner or other staff. Example: "Scribed for Dr. X by name of the scribe and title" with the date and time of the entry.
- The physician or practitioner must then authenticate the entry by signing, dating and timing (for deemed status purposes) it. The scribe cannot enter the date and time for the physician or practitioner. (RC.01.01.01 and RC.01.02.01).
- Although allowed in other situations, a physician or practitioner signature stamp is not permitted for use in the authentication of "scribed" entries-- the physician or practitioner must actually sign or authenticate through the clinical information system. (RC.01.02.01).
- The authentication must take place before the physician or practitioner and scribe leave the patient care area since other practitioners may be using the documentation to inform their decisions regarding care, treatment and services. (RC.01.02.01 and RC.01.03.01).
- Authentication cannot be delegated to another physician or practitioner. The organization implements a performance improvement process to ensure that the scribe is not acting outside of his/her job description, that authentication is occurring as required and that no orders are being entered into the medical record by scribes. (RC.01.04.01).

[1] Joint Commission guidelines

Risk Pearls: July 2017

By Justin Joy, JD, CIPP

Tempting as it may be, think twice before accessing medical records if you receive a notice of intent to sue or are served with a lawsuit. An electronic health record (EHR) system tracks activities and records the information in metadata—the "data about data"—or in audit logs. This recorded information may include details about the date and time a record was accessed, who accessed it, and in certain circumstances, how long the record was viewed. While this "digital footprint" is largely invisible in day-to-day operations, a lawyer for a patient could have an interest in which records a defendant provider reviewed after learning of a lawsuit, which could then lead to more questions about the reasons the records were viewed. Whether inadvertent or intentional, alteration of a medical record (even to correct an earlier typographical error or misstatement) could have serious negative implications on the defense of a lawsuit. Because there is an obligation of all parties to preserve evidence once they are in reasonable anticipation of litigation, alteration or destruction of a medical record could lead to a claim of attempting to conceal evidence. Such actions can lead to court sanctions and possibly eliminate the protection of statutory damage caps. The burden of disproving an alteration was intentional could, at best, provide an unpleasant distraction from the defense of an otherwise defensible claim.

The take-away here: A record cannot be altered if it is not accessed.
