

ClaimsRx

clinical & risk management perspectives

October 2009

Electronic Health Records: Recognizing and Managing the Risks

CME Information

Sponsored by:
NORCAL Mutual Insurance Company.

NORCAL Mutual Insurance Company is accredited by the Accreditation Council for Continuing Medical Education to provide continuing medical education for physicians.

Method and Medium

To obtain CME credit, read the enduring material article, and complete and return the attached activity Evaluation and CME Attestation Form no later than the expiration date indicated below.

Original Release Date: October 2009

Expiration Date: October 31, 2010

Learning Objectives

By reviewing the cases presented in this course and implementing the risk management recommendations, you will increase your ability to:

- Adopt and adhere to electronic communication and documentation standards.
- Utilize the EHR system productively while continuing to implement patient safety practices, such as double-checking medication dosages, using an effective follow-up system and reviewing records for accuracy.
- Develop policies and procedures specifically related to training in the safe use of the EHR system.

Target Audience

All providers

Credit Designation Statement

NORCAL Mutual Insurance Company designates this educational activity for a maximum of *1 AMA PRA Category 1 Credit*.™ Physicians should only claim credit commensurate with the extent of their participation in the activity.

Disclosure Policy

As an ACCME accredited provider, NORCAL Mutual Insurance Company requires planners, reviewers or authors who influence or control the content of a CME activity to disclose financial relationships (of any amount) they have had with commercial interests associated with this CME activity during the year preceding publication of the content. Any identified conflicts of interest are resolved prior to the commencement of the activity.

Disclosures

Individuals involved in the planning, reviewing or execution of this activity have indicated they have no relevant financial relationships to disclose.

Editor

Mary-Lynn Ryan

Consulting Risk Management Specialist, NORCAL

Content Advisors

David R. Holley, MD

Chairman, NORCAL Board of Directors

Harry B. Richardson, Jr., MD

Vice Chairman, NORCAL Board of Directors

William R. Vetter, MD

Secretary, NORCAL Board of Directors

Patricia A. Dailey, MD

NORCAL Board of Directors

Michael Stephens

NORCAL Board of Directors

Newell E. Warde, PhD

NORCAL Board Advisory Council

Executive Director, Rhode Island Medical Society

James Sunseri

President & CEO, NORCAL

Stephen M. Farber

Vice President, Risk Management, NORCAL

Neil Simons

Vice President, Underwriting-Marketing-Policyholder Services, NORCAL

Jane Tishkoff, Esq.

Associate Vice President and

Assistant General Counsel, NORCAL

Marlene Nazarey, RN, MSN

Manager, Risk Management, NORCAL

Dustin Shaver

Manager, Risk Management, NORCAL

Paula Snyder, RN, CPHRM

Manager, Risk Management, PMSLIC

John Resetar

Supervisor, Claims Department, NORCAL

Planners

Jo Townson

Risk Management Specialist, NORCAL

Sonia Rutherford

Risk Management CME Program Services

Coordinator, NORCAL

Introduction

Electronic health records (EHRs) hold great promise of improving patient safety and decreasing medical liability exposure, but their use is creating a variety of new risk management and patient safety issues. Some of these issues are directly associated with EHRs (e.g., providers disregard warnings generated by the EHR), but many of the risk concerns associated with EHRs are analogous to problems that currently exist in paper documentation systems.

In this month's *Claims Rx* we present a number of shorter-than-usual case studies that exemplify various aspects of unsafe EHR documentation and communication practices. The scenarios are based on NORCAL closed claims, facts presented in appellate opinions,

research findings and the observations of NORCAL Risk Management Specialists.

What many of the examples show is that EHRs do not eliminate many of the dangerous documentation and communication practices that have historically led to patient injury and malpractice lawsuits. Consequently, while it is important to address new issues that arise with EHRs, many of the risk management recommendations that apply to a paper-based documentation system remain valid.

This *Claims Rx* will discuss the risks associated with various aspects of EHRs and will provide guidance for instituting policies and procedures designed to enhance the quality and safety of patient care, while diminishing professional liability risk.

Federal EHR Incentive Program

In February of this year, President Barack Obama signed the American Recovery and Reinvestment Act (ARRA), which sets aside \$17.2 billion dollars of the economic stimulus package for incentive payments to Medicare and Medicaid providers who implement EHRs according to standards that are projected to be available by the end of 2009.*†

The payouts begin in 2011. Early adapters who can demonstrate “meaningful use” of EHRs (among other features, the system must have e-prescribing, can connect with other EHRs and can report clinical quality measures) are eligible for the highest reimbursement amounts. The reimbursement amount diminishes by year, up through 2014. For Medicare providers, the payout maximum is \$44,000 over five years. For Medicaid it is nearly \$64,000 over six years. In 2015, providers who cannot demonstrate “meaningful use” may have their Medicare rates diminished by 1%. This increases to 2% in 2016 and 3% in 2017 and may rise even higher in future years. Medicaid does not have a similar penalty structure.†‡

As could be expected, EHR vendors are aggressively marketing their products. It can take over a year to get an EHR system up and running, so being eligible for the 2011 stimulus payment could be a real challenge for someone who waits too long to make the initial EHR investment. It is important, however, to consider several aspects of the incentive payment legislation before investing in an EHR for the purpose of collecting a 2011 reimbursement. For example, the rules coming out at the end of the year are supposed to further define “meaningful use” and are expected to detail the nature of physician-to-physician data exchange requirements, describe clinical quality measures that must be reported to the U.S. Department of Health and Human Services (HHS) and describe the process of certification.*

Despite the possible loss of the first incentive payment, providers are urged to carefully consider which EHR is appropriate for their practice and allow an appropriate amount of time for training and rolling out the new system.

Federal EHR Incentive Program (continued)

EHR Implementation Resources

A variety of organizations provide further information on the various aspects of converting from paper to electronic records, including:

Joint Commission

The Joint Commission published "Safely implementing health information and converging technologies," Sentinel Event Alert 42, December 11, 2008, which makes patient safety recommendations related to EHR implementation. It is available on the Joint Commission Web site at: www.jointcommission.org/SentinelEvents/SentinelEventAlert/sea_42.htm (accessed 8/24/2009).

American Academy of Family Physicians (AAFP)

Through its Center for Health Information Technology Web site, the AAFP offers advice on every step of an EHR conversion: www.centerforhit.org (accessed 8/24/2009).

References

* Marilyn Lamar, Esq. "Embracing benefits, facing risks with EHR technology." Presented by ASHRM on 8/4/2009.

† Stephen H Carson, MD. Electronic Health Record: Beware. San Joaquin Physicians. Summer 2009.

‡ Robert Lowes. Experts Offer EHR Advice in Light of New Federal Incentives. May 14, 2009. Available on the Medscape Web site at: www.medscape.com (accessed 8/24/2009).

Data Entry Errors

EHRs may decrease errors caused by unintelligible handwriting, but they cannot be expected to eradicate human error. Providers are encouraged to question EHR information that does not seem right (e.g., abnormally high medication dosages, radiographic images that are not consistent with the patient's anatomy, etc.) and attempt to reconcile conflicting information.

Saving Images in the Wrong Patient's Chart

Just as an image can be misfiled or lost in a paper system, it can be misfiled in an electronic one. However, as the following case shows, it can be less obvious that an image has been misfiled in an electronic system.

Case Study

Patient #1 and patient #2 both presented to the Emergency Department (ED) complaining of abdominal pain. CT scans of the abdomen and pelvis were completed for both patients. A radiology tech mistakenly gave patient #2's images the identification number assigned to patient #1 and uploaded the images into the

Picture Archiving Computer System (PACS). A short time later, the tech realized his mistake and called the on-duty teleradiologist to tell him about the mistake and request that the mislabeled images be deleted from the system. However, the on-duty teleradiologist did not have access to delete images from the PACS; this had to be done by the PACS administrator. The tech then corrected the labeling problem and sent the images out to the teleradiology service for a preliminary review and resent the correctly labeled images to the PACS. Patient #1's PACS file now contained both his own and patient #2's images. A few days later the tech told his supervisor about the mislabeling, and assumed that the supervisor would remedy the problem. Pursuant to hospital policy, the tech should have immediately contacted the PACS administrator.

The teleradiology service reported that patient #1's CT scan was normal. Patient #2's CT scan, however, showed a large tumor (about the size of a grapefruit) on the patient's kidney. The service faxed the reports to the radiology department at the hospital.

(continued on page 4)

The next morning, the on-duty radiologist reviewed the PACS images from the night before. He disregarded the teleradiology service reports because they did not correspond to what he saw in the PACS. Because patient #2's scan had been completed before patient #1's, patient #2's images were the first series in his file. The on-duty radiologist noted the large tumor and dictated a note. Because patient #2's images still carried patient #1's identification number, the radiologist's report was assigned to patient #1.

Patient #1 was subsequently seen by a number of specialists for the supposed tumor on his kidney. Seven days after the CT scan, he underwent a nephrectomy. During the surgery, no mass could be positively identified on his kidney by his surgeons. Postoperatively, no tumor was identified in the removed kidney and pathology returned benign.

(Please note, once the filing mistake was recognized, patient #2 was notified and underwent a timely and successful nephrectomy.)

Discussion

A combination of system problems and communication issues led to this patient's unnecessary surgery. It probably never would have occurred if the tech had either followed the policy of alerting the PACS administrator of his error or had had the capacity to delete an image that he had mislabeled. He should have known that neither the teleradiologist nor his immediate supervisor would be able to delete images from the PACS.

The problem was compounded by the radiology department's alteration of the EHR system. In its altered state, two series of images automatically opened up on two viewing screens — one screen showing the “scout” films and the other screen showing the cuts. The radiologists needed to click on a small button on one of the monitors marked “series” to see any other films. In this case, the radiologist did not suspect any other films were taken, so he had no reason to click on the “series” button.

Another problematic issue was the radiologist's failure to look further into why the PACS images he saw were entirely inconsistent with the fax report he received

from the radiology service. He was in the habit of disregarding the service's reports because he thought they were consistently inaccurate.

Lastly, the surgery team went through with the nephrectomy despite the surgeon recognizing that the patient's anatomy did not correspond to the CT image on the wall that showed a very large tumor.

Risk Management Recommendations

- If something in the EHR does not make sense, double check it. Do not assume that the information is correct simply because it is in the EHR.
- If you make a mistake in a person's record and have to depend on someone else to correct it, go back to the patient's record to confirm that the record has been appropriately corrected.
- Continually assess whether EHR reconfigurations increase patient safety and reduce professional liability risk exposure; if they don't, find alternative means to achieve needed alterations to the system.
- Ensure that staff and clinicians are aware of EHR policy and that they are following it.

Checking the Wrong Box

In the following case, the appearance of the computer screen probably played a role in the medication error.

Case Study

A patient presented to his primary care physician (PCP) for the treatment of headaches and episodes of altered consciousness. The PCP prescribed amitriptyline at 10 mg nightly. The PCP told the patient to escalate the dosage by 10 mg every three to four days until the pain was relieved, but not to exceed 50 mgs without consulting him. When creating the prescription, the PCP intended to check off the 10-mg box in the computerized physician order entry (CPOE), but inadvertently checked the 100-mg box, which was right above it. In the medication instructions section, he indicated that five pills could be taken per night, so the patient would not have to return to the pharmacy and pay an additional co-pay if he ultimately needed the larger dose.

The pharmacist had noticed that the dose seemed high and requested that a call be made to the PCP prior to it being dispensed. A nurse at the PCP's office picked up the call, and because she was very busy that day, told the pharmacy to dispense the medication as it had been ordered — she did not check the dose. Three days later, the patient took five of the 100-mg pills together. Early the next morning, the PCP was contacted by an emergency department (ED) physician who reported that the patient was in the ED reporting dizziness, an altered state of consciousness, an inability to coordinate his movements and a rapid heartbeat. He was further informed by the ED physician that the patient had taken five 100-mg amitriptyline tablets. The PCP then checked the patient's record and realized his mistake.

Discussion

In this case, the nurse assumed that because the dosage had come from the system, it was correct. As this case indicates, however, a typographical error can be as dangerous as illegible handwriting. It is important to recognize problems with an EHR and attempt to get them solved so they are less likely to result in treatment errors. For example, in this case, the provider could contact his EHR vendor and attempt to work out a way to move the check boxes associated with dosage amounts further apart on the drug ordering screen or have a pop-up box that confirms the ordered medications before closing out of the record.

General Medication Transcription Risk Management Recommendations

In addition to appropriately following up on dosage questions (which the nurse in this case obviously did not do), an EHR system should be configured to apply the risk management tactics that apply to paper records, and when such functions are not available, paper-record tactics should be used in making entries in the electronic record:

- Include a brief notation of the purpose on all prescription orders (e.g., for cough), unless considered inappropriate by the prescribing physician.
- Record all prescription orders in the metric system except for therapies that use standard units such as insulin, vitamins, etc.

- Include age and, when appropriate, weight of the patient on the prescription or medication order.
- Include drug name, exact metric weight or concentration and dosage.
- Always precede a decimal expression of less than one with a leading zero.
- Do not use a terminal or trailing zero after a decimal.
- Avoid using abbreviations including those for drug names (e.g., spell out “unit” and “international unit” rather than writing “U” or “I.U.”; use “daily” or “every other day,” whichever is applicable, not “q.d.” or “q.o.d.”).
 - The Institute for Safe Medication Practices (ISMP) publishes a list of unacceptable abbreviations and symbols, which is available on the ISMP Web site at: www.ismp.org (accessed 8/24/2008).

Typing the Wrong Dose

Although some EHR systems flag medication doses that are abnormally high, as the previous and the upcoming case studies show, there are dosage errors that will slip through the cracks.

Case Study

A 75-year-old man presented to a cardiologist's office to establish care. He had a history of moderate pulmonary hypertension, hyperlipidemia, chronic gout, glaucoma, cholecystectomy, and presbycusis. The patient had been taking various medications, including a 0.25-mg Xanax tablet prior to scheduled appointments to relieve his anxiety.

The medical assistant (MA) responsible for rooming the patient took the patient's copy of his medication list and noted that the patient was taking “Xanax (alprazolam) 2-mg tabs prn” in the electronic medical record. The prescription for Xanax 2 mg tabs prn was “refilled” at the patient's pharmacy.

Three months later, the patient presented to his ophthalmologist. Prior to the appointment, he took a 2-mg Xanax tablet to alleviate his anxiety. On his way home he fell asleep behind the wheel and crashed into a tree. After the accident, the physician reviewed the

(continued on page 6)

patient’s medical record and recognized that the MA had entered Xanax “2 mg tabs prn.” Unfortunately, the physician had gotten into the habit of signing off on the medical assistant’s entries without really reviewing them.

Discussion

The foregoing case example shows that caution must be used when recording patient information, even when it is captured and entered into an EHR. The physician in this case relied on an MA to accurately transcribe the patient’s medication list into the EHR, and there was no verification process in place. Once the original entry made it into the patient’s record, it was never reviewed. Transcription errors are often caused by clerical staff members who misunderstand an order or have difficulty reading an original document because of illegibility.¹

According to one study, multifaceted intervention involving providers and patients can significantly improve medication list discrepancies in an electronic medical record. Essential interventions in the study included mailing letters to patients before appointments to remind them to bring all medication bottles or an updated medication list to their clinic visit and having the patient verify the most recent medication list in the electronic medical record. Although these methods significantly reduced discrepancies, they did not completely eliminate them. The study authors recommended further system designs such as medication cards and/or nurse- or software-aided collection of medication lists from patients before visits.²

Risk Management Recommendations

- Ensure that a licensed healthcare professional double-checks medications transcribed into an electronic medical record.
- Institute procedures that regularly update and reconcile patient medication lists.
- Mail letters prior to appointments asking patients to bring in all prescription medications and over-the-counter medications to appointments.

- Generate an electronic medication list and compare the electronic list to the medication bottles while the patient is in the office.
- If patients do not bring in medication bottles, enlist the patient to ensure the accuracy of the electronic medical record medication list.
 - Ask the patient to compare the medication list generated from an electronic record with medication bottles at home.

System-Assisted Documentation

The issue of incomplete/inaccurate documentation takes a variety of forms in the EHR arena. Functions in an electronic record that were designed to save time have created a whole new set of risk management issues.

Case Study

A 50-year-old woman presented to the ED complaining of neck and leg pain. The ED physician did his exam from the doorway of the patient’s room using his tablet PC. He checked off items on the electronic “T-sheet” while he asked a few basic questions. It took him less than one minute. Out of curiosity, an ED nurse who was present reviewed his documentation. She found that there was a “comprehensive assessment” documented.³

Discussion

The foregoing case study provides an example of documentation that uses a template to self-generate certain aspects of the patient’s record. This EHR function (also referred to as an “exploding note”) allows users to pull up a template for a particular condition and then check boxes indicating normal or abnormal values or observations. An examination note in paragraph form is then produced for the EHR. In the foregoing case, the ED physician was engaging in a practice that may be considered fraudulent billing by the Centers for Medicare and Medicaid Services (CMS). From a medical liability standpoint, if this physician’s treatment came into question, it would be difficult for him to convincingly support the adequacy of his assessment. If self-populating forms are used, it is important to go through the entire form and ensure that the note that has been created accurately reflects the patient’s condition.

A practice referred to as “cloning” can result in similar documentation inaccuracies. Cloning refers to copying information from an earlier exam and “pasting” the information into the record for a current exam. This can occur in the same patient’s chart or between different patients. Although it is considered appropriate to copy a complex medical history from an earlier exam, providers should not use “cloned” content for a patient’s history of a present illness, the exam or the medical decision-making process — and particularly not for a different patient.⁴ Using the EHR to document treatment that did not occur or to inappropriately clone notes diminishes the integrity and usefulness of the medical record.

Providers are under pressure to see as many patients as possible while keeping the “customer” satisfied. It is important to remember that the primary function of an EHR is to manage data — it does not replace complex decision-making or face-to-face contact with the patient. While taking advantage of time-saving features provided by an EHR might be tempting, the issue of patient safety should remain central.

Breach of Confidentiality of Medical Information

The breach of confidentiality of medical information happens with paper medical records. EHRs, however, allow for a level of breach that is inconceivable at the paper-record level.

*Case Study*⁵

An MA observed her sister-in-law enter an examination room. Against clinic policy, the MA accessed the patient’s medical record and discovered that the patient had requested testing for sexually transmitted diseases because she had a new sex partner. She also learned that the patient was diagnosed with a sexually transmitted disease. Later that week, the MA and her sister created a MySpace page that included the patient’s picture and the sexually transmitted disease information from her medical record.

Discussion

The foregoing case example was taken directly from a 2009 Minnesota Appellate Court opinion. It exemplifies the

ease with which a person with bad intentions can access an electronic medical record and publicize confidential information. Even individuals with benign intentions technically violate patient privacy when they casually browse through patient records for no medical purpose.

Having a security policy that includes password usage is a first line of defense against unauthorized access to patient medical information. Unfortunately, a password alone does not protect confidentiality when the password holder is untrustworthy or has poor judgment. There is probably no fail safe way to keep medical information confidential, but there are ways to make it more difficult for clinicians and staff members to inappropriately access information, including:⁶

- Add additional layers of access restrictions (for example, in addition to a password, the person accessing the record must have a particular job or must be part of a particular team of providers).
- Implement two-factor user authentication — add a second, physical proof for access. (A bank ATM card is an example of a widely used form of two-factor authentication. It requires the combination of a PIN and a valid card for access.)
- Put protocols in place that define which staff members need access to the EHR and the level of access that is appropriate.
- Do not allow password sharing.
- Change passwords frequently.
- Review audit reports weekly or monthly to show who has accessed the medical records, during which hours and for which functions.
- Create a medical information confidentiality policy.
- Consistently discipline people who violate confidentiality policies.

Because technology continues to become more sophisticated, it is important to regularly reevaluate the applicability of security protocols. Communicate regularly with vendors and IT staff to ensure state law and HIPAA health information confidentiality compliance.⁷

“Curbside” Consultations

Email conversations between providers add a new dimension to the risks associated with “curbside” consultations.

Case Study

A 64-year-old uninsured man was under the care of a family practitioner for multiple health issues, including an aortic murmur, high blood pressure, high cholesterol and diabetes. A CT scan revealed an aortic thrombus. The physician emailed the scan and report to a friend who was a vascular surgeon, asking for treatment recommendations. The surgeon recommended that an angiogram be performed to further evaluate the thrombus. The physician replied back that the patient was uninsured and that an additional test would be too expensive. As an alternative, the surgeon suggested the patient be placed on warfarin. The physician “cut and pasted” the surgeon’s recommendation from the later email into the patient’s medical record. Based on the vascular surgeon’s recommendation, he initiated warfarin therapy at 2.5 mg per day. He conducted routine Prothrombin Time (PT) and International Normalized Ratio (INR) testing. After five months of therapy, the patient’s dose was set at 10 mg per day. One repeat CT scan was done after four months of therapy, revealing that a thrombus was still present at the same location. The patient could not afford additional testing, so the physician never ordered another CT scan.

Two years after the patient had started on warfarin a series of unfortunate events led to him dying shortly after being hospitalized for warfarin overdose.

Discussion

Plaintiff’s experts were critical of both the family practitioner and vascular surgeon for the patient being placed on anticoagulation therapy without a formal consultation. They believed that, at a minimum, a vascular surgeon needed to review the patient’s medical records and films to give an opinion regarding the patient’s condition. The vascular surgeon had no idea that his casual recommendation would become part of the patient’s chart. It was additionally disturbing to find that his initial recommendation for an angiogram did not get “pasted” into the patient’s chart.

Risk Management Recommendations

- Formally consult with specialists when necessary and document consultations in the patient’s chart.
- Recognize that informal consultations are based on incomplete information and take place without the benefit of review or examination of the patient. Do not replace a formal consultation with a “curbside” consult.
- When emailing colleagues, realize that correspondence may become part of the patient’s medical record.
- Label the email with a statement regarding whether you are providing a formal consultation.

Inadequate EHR Training

Inadequate training can increase liability risk, diminish patient safety, decrease productivity and result in user frustration. Intensive training on the EHR is particularly important during transition from a paper record, but it is also necessary on an ongoing basis to ensure user competency. As the following case shows, a healthcare entity must not only ensure employee EHR competency, but it should also ensure the EHR competency of independent contractors who use the system.

Case Study

On July 1, 2006, the patient, a 45-year-old man with a history of thyroid cancer, presented to the ED complaining of groin pain. A chest x-ray and a CT scan of the abdomen and pelvis were ordered. Radiologist #1 reported that the chest x-ray showed a 3-4-mm nodular opacity in the left *upper* lobe of the lung, which he thought might be a small granuloma. Radiologist #2 noted a 9-mm pulmonary nodule in the left *lower* lobe of the lung on the CT Scan. Due to a series of miscommunications, these results were entered directly into the patient’s electronic record and his PCP was never informed of the results.

Months later, radiologist #3 interpreted another chest x-ray and noted a faint nodular density in the left *upper* lobe of the lung. Radiologist #3 thought this was equivocal and so informed the PCP. After speaking with radiologist #3, the PCP logged onto the radiology department’s Web site. He brought up the patient’s July 1

chest x-ray, but could not see any irregularities. He then attempted to access the July 1 abdominal CT images, but he had trouble manipulating the icons. He was, however, able to access the abdominal CT report. Because much of the *upper* lobe overlaps the lower lobe, the PCP assumed that the nodule mentioned in the CT report was the upper lobe density that radiologist #3 had told him was equivocal. Three years later the patient was diagnosed with lung cancer in the *lower* left lobe, where the density had been identified three years earlier.

Discussion

This claim was complicated by the fact that the hospital was transitioning to an electronic medical record system. Unfortunately, the PCP did not obtain training on the system. His inability to fully access his patient's information contributed to his failure to adequately follow up on the 2006 chest x-ray and CT scan results.

Risk Management Recommendations

- Have a transition plan in place that is realistic and adequately communicated to any provider who treats patients at your facility or refers patients to your facility for testing or treatment.
- Provide adequate training and technical support.
 - If providers are expected to use an electronic medical record system, make available training opportunities with ongoing support.
- Ensure healthcare team member EHR proficiency.
 - Conduct audits and follow-up on identified weaknesses.
 - Provide refresher courses as necessary.
- Provide an environment where healthcare team members feel empowered to request assistance.
- Regularly assess and monitor errors and near misses. Evaluate the cause of the problems and address them.⁷

Failure to Check EHR or Email Inbox

A problem minimally related to the electronics of communication, but more related to an individual's personal practice, is not regularly checking one's EHR and email inbox for test results. The issue is akin to not dealing with an inbox overflowing with paper. An interesting recent study found that having an EHR that delivers all test results via email in offices without adequate follow-up processes actually can increase the chance that a physician will not receive significant results. In other words, in a paper-system office with inadequate follow-up processes, the chances of a test result being noticed on a physician's desk are greater than are the chances of that test being discovered in a physician's EHR or email inbox.⁸

If your practice is using the EHR or email for test result delivery, it is important to have a policy in place that describes how frequently providers must check their inboxes and the process by which results are then communicated to the various parties who need to see them. For a more detailed discussion about test result communication, see the May 2009 *Claims Rx* entitled "Failure to Appropriately Communicate Abnormal Test Results," which is available on the NORCAL Web site at: www.norcalmutual.com/publications/claimsrx/may_09.pdf (accessed 8/25/2009).

(continued on page 10)

Patient-Physician Email Correspondence Guidelines

The use of email is becoming more common between providers and their patients. Various medical associations have published guidelines for physician-patient electronic communication. Included below are a combined selection of email correspondence recommendations from the American Medical Association and the California Medical Association:*

- Establish a turnaround time for messages.
- Use an automatic reply function to acknowledge receipt of the patient's message and to warn patients against emailing regarding urgent matters.
- Inform patients about the information privacy and security limitations of email.
- Inform patients about who (other than the provider) is responding to emails.
- Retain and integrate electronic and/or paper copies of email communications with patients in their medical record.
- Establish policies that delineate the types of transactions (prescription refill, appointment scheduling, etc.) and sensitivity of subject matter (HIV, mental health, etc.) that are permitted in email correspondence.
- Tell patients to indicate their main objective (e.g., prescription refill, billing issues) in the subject line of the message.
- Instruct patients to include their name, insurance plan, and patient identification number either in the subject line or in the body of the message.
- Inform patients when their request has been completed.
- Instruct patients to use an autoreply feature to acknowledge receipt of the provider's message.
- Develop email retention, archival and retrieval policies and procedures.
- Do not send group mailings where recipients are visible to each other; use a blind-copy email function.
- End each email message with the provider's full name, contact information, reminders about medical information security and warnings about email communication for emergencies.
- Request that patients send concise messages.
- If email messages from a patient become lengthy, confusing or if the correspondence is prolonged, ask the patient to discuss the issue in person or on the telephone.
- Advise patients that abiding by the email policies is a condition of continued email communication.

Because email becomes part of the medical record, and even if deleted it remains on the system, providers are encouraged to utilize the same conventions that would be employed for any other patient communication. For example, avoid anger, sarcasm, harsh criticism, and libelous references; use proper grammar; and check spelling.

Resources

* AMA Guidelines for Physician-Patient Electronic Communications. Available on the AMA Web site at: www.ama-assn.org/ama/pub/about-ama/our-people/member-groups-sections/young-physicians-section/advocacy-resources/guidelines-physician-patient-electronic-communications.shtml (accessed 8/24/2009).

† Physician Web sites, internet advice and email. CMA On-Call Document #0823. January 2009. Available on the California Medical Association Web site at: www.cmanet.org (accessed 8/24/2009).

Turning Off the System's Warning Messages

Case Study

Isaac, et al. performed a retrospective analysis of 233,537 medication safety alerts generated by 2,872 clinicians in Massachusetts, New Jersey, and Pennsylvania who used a common electronic prescribing system. From January 1, 2006, through September 30, 2006, the system warned physicians nearly 230,000 times about potential drug interactions. Ninety percent of the time the physicians who received these warnings proceeded as if the alert had not appeared.⁹

Discussion

Most EHRs offer medication alerts. The objective of these alerts is to warn the person prescribing or ordering a medication of potential adverse drug interactions, allergic reactions, etc. Unfortunately, EHR alert technology has not developed to the point of full utility. As the study above indicates, a majority of physicians turn off or routinely override the alert function because it adds little value to them or their patients. As the technology catches up to the needs of the people who must use it, providers are encouraged to be cautious when disabling or overriding a system's alert functionality. In the event of malpractice litigation arising from a medication error, the record of alerts that have been turned off or selectively overridden may be difficult to explain to a judge or jury, especially when heeding an ignored warning could have prevented the patient's injury.¹⁰

Risk Management Recommendations

- Work with vendors to create an alert system that is as usable as possible.
- Develop a system of alerts that allows clinicians to determine their urgency and relevancy.

- Review which alerts are overridden and determine whether these need to be "hard stops" (alerts that cannot be overridden). Document the decision-making process.⁷
- If you do not use the alert system of an EHR, use an alternative system for determining whether the patient would be exposed to allergy or drug interaction risks. Document the result of your efforts.

Failure to Obtain Buy-in from Every Member of the Healthcare Team

Some providers will not make the change to EHR, regardless of the incentives offered or the penalties assessed. What is an individual decision for one, however, can affect an entire group's recordkeeping practice. There are valid arguments on both sides of the EHR implementation debate, but if the implementation decision has been made and one or more providers refuse to use it, the issue cannot be ignored. Note-taking followed by later transcription can lead to delays and/or inaccuracies. Some practices have managed this situation by assigning a "scribe" to a physician who either cannot or will not use an EHR. Although this would obviously be an expensive way to manage the situation, it highlights the fact that there are creative ways to work around buy-in problems.

Conclusion

Because of the complexity of the many solutions and options available and the unique needs of each practice, planning, research and training are critical to the successful conversion from paper to electronic records. Providers are encouraged to implement and appropriately update policies and procedures that address the liability and patient safety risks that are particular to these new and constantly improving technologies, while continuing to apply risk management strategies that have been effective in a paper-based system.

CPOE (Computerized Physician Order Entry) Risks Identified in a Recent Study

A 2005 *JAMA* article discusses a study that focused on medication errors facilitated by CPOE in a major urban tertiary-care teaching hospital with 750 beds, 39,000 annual discharges, and a widely used CPOE system operational there from 1997 to 2004. The authors found that the CPOE system at this hospital facilitated 22 types of medication errors, as illustrated by the following:

- Physicians relied on the CPOE displays to determine the minimal effective or usual doses, but those doses were based on the pharmacy's warehousing and purchasing decisions, not on clinical guidelines. For example, where a usual dosage was 20 or 30 mg, the pharmacy would stock 10-mg doses, which resulted in 10-mg units being displayed on the CPOE screen. Physicians then ordered 10-mg doses for patients, mistakenly believing that it was the usual dosage.
- Physicians ordered increased or decreased doses of medications without discontinuing current dose because they mistakenly believed that ordering the new dose would automatically discontinue the current dose in the system.
- Physicians ordered medications that were associated with a particular procedure or test, but if the procedure or test was cancelled, the system did not automatically cancel the medication. Consequently, patients received unnecessary medications.
- Because medication charting was cumbersome and the screen displays were fragmented, immediate orders and "give as needed medications" (P.R.N.) were often not entered into the system and not cancelled as directed. This resulted in patients receiving unintended doses.
- Because reapproval stickers were placed in the paper chart and physicians primarily used the CPOE to order antibiotics, unintentional gaps occurred in patient antibiotic therapy.
- The CPOE required physicians to identify diluents for administering antibiotics, but the physicians were not aware of interactions between some diluents and antibiotics. This generated precipitates and other problems.
- Allergy information was delayed because physicians ignored warnings and depended on pharmacists for checking drug allergies.
- Physicians selected the wrong patient record because the names were close together, the font was small, every screen did not contain the patient's name and patients were listed alphabetically, instead of by teams or rooms.
- The wrong medication was ordered because the patient's medication information was not synthesized on one screen. Getting all of the medication information sometimes necessitated going through 20 screens.
- Because a physician was not logged out of a patient's record, the patient whose record was still active got a medication intended for a different patient.
- Because the EHR cancelled preoperative orders and required numerous steps to activate orders following surgery, postsurgical medication was delayed.

CPOE (Computerized Physician Order Entry) Risks Identified in a Recent Study (continued)

- Because of system “crashes” and maintenance, drug ordering was delayed. If a patient was moved while the system was down, medications went to the new patient in the patient’s former room.
- A cumbersome interface made contemporaneous drug administration recording difficult, resulting in drug administration being charted at the end of the shift and consequently providing physicians with inaccurate information about when the medication was administered.

Based on their findings, the authors made the following recommendations:

- Do not direct clinical actions with CPOE if it causes patient care to deteriorate.
- Examine the technology to determine if it is working effectively.
- Fix the technology if it is counterproductive.
- When a medication error occurs, look for the weakness in the way the system works instead of assuming the error was the result of human error.
- Expect and plan for revisions and quality improvement.

Reference

Koppel R., et al. Role of Computerized Physician Order Entry Systems in Facilitating Medication Errors. *JAMA*. 2005;293(10):1197-1203.

Endnotes

- ¹ Leape LL, Bates DW, Cullen DJ, et al. Systems analysis of adverse drug events. *JAMA*. 1995;274:35-43.
- ² Varkey P, Cunningham J, Bisping S. Improving Medication Reconciliation in the Outpatient Setting. *The Joint Commission Journal on Quality and Patient Safety*. May 2007. Volume 33 Number 5.
- ³ Case study based on “Templated Charting—The Slippery Slope to Fraudulent Documentation,” Friday, October 12, 2007. Available on the ERMurse Blog at : <http://ermurse.blogspot.com/2007/10/templated-charting-sslippery-slope-to.html>. (accessed 8/24/2008).
- ⁴ Compliance Risks Grow with Electronic Medical Record Systems. www.aishealth.com/Compliance/ResearchTools/RMC_Compliance_Risks_EMRs.html (accessed 8/24/2009).
- ⁵ Case study based on *Yarb vs. Fairview Clinics, et al.* 767 N.W.2d 34; 2009 Minn. App. LEXIS 117 (2009).
- ⁶ HIPAA Security Guidance for Remote Use. Available on the U.S. Department of Health and Human Services Web site at: www.cms.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal122806rev.pdf (accessed 8/24/2009).
- ⁷ Safely implementing health information and converging technologies. Sentinel Event Alert 42, December 11, 2008. Available on the Joint Commission Web site at: www.jointcommission.org/SentinelEvents/SentinelEventAlert/sea_42.htm (accessed 8/24/2009).
- ⁸ Casalino R, et al. Frequency of Failure to Inform Patients of Clinically Significant Outpatient Test Results. *Arch Intern Med*. 2009;169(12):1123-1129.
- ⁹ Isaac T, Weissman S, Davis R, Massagli, Cyruklik A, Sands D, Weingart S. Overrides of Medication Alerts in Ambulatory Care. *Arch Intern Med*. 2009;169(3):305-311.
- ¹⁰ Shay E. Electronic health records in litigation. Published September 2008. Available on the Physician’s News Digest Web site at: www.physiciansnews.com/law/908shay.html (accessed 8/24/2009).



MyCME

A Bright Invention from NORCAL

Introducing MyCME from NORCAL Mutual. Review our wide array of risk management resources and services. Register for and complete CME courses at your convenience. Submit your Attestation Form online. Print transcripts and certificates... everything from one easy-to-navigate website.

Learn more at www.norcalmutual.com/cme
or call 800.652.1051, ext 2244.



*Our passion protects
your practice*



560 Davis Street, Suite 200
San Francisco, CA 94111-1966

Prsrt. Std
U.S. Postage
PAID
Permit #751
San Diego

Inside . . .

Electronic Health Records:
Recognizing and Managing the Risks

ClaimsRX

clinical & risk management perspectives
October 2009

New CME Podcast available
at www.norcalmutual.com.

Now you can earn CME credit wherever you are with *Complex Regional Pain Syndrome* – a new CME podcast available exclusively from NORCAL Mutual. Go to www.norcalmutual.com and click on podcast to download and listen to this new CME activity.

©2009 NORCAL Mutual Insurance Company.
Reproduction permissible with written permission and credit.

Direct inquiries to:
NORCAL Mutual Insurance Company
Risk Management Department
560 Davis Street, Suite 200
San Francisco, CA 94111-1966
(800) 652-1051

The information in this publication is obtained from sources generally considered to be reliable; however, accuracy and completeness are not guaranteed. The information is intended as risk management advice. It does not constitute a legal opinion, nor is it a substitute for legal advice. Legal inquiries about topics covered in this publication should be directed to your attorney.

Guidelines and/or recommendations contained in this publication are not intended to determine the standard of care, but are provided as risk management advice. Guidelines presented should not be considered inclusive of all proper methods of care or exclusive of other methods of care reasonably directed to obtain the same results. The ultimate judgment regarding the propriety of any specific procedure must be made by the physician in light of the individual circumstances presented by the patient.

Visit NORCAL Mutual on the Internet at www.norcalmutual.com.

Claims Rx
Evaluation and CME Attestation Form
Electronic Health Records: Recognizing and
Managing the Risks

Release Date: October 2009
Expiration Date: October 31, 2010

In order to receive CME credit,* you must fill out this form in its entirety and return it to NORCAL Mutual by the expiration date above. For instant access to your CME certificate, go to www.norcalmutual.com/cme, log-in to MyNORCAL and click on MyCME. You may access this enduring material and submit the form electronically. Alternatively, you can mail or fax this (paper) form to receive your CME certificate in 7-10 business days.

Name: _____

Address: _____

Phone: _____ Email: _____

NORCAL Mutual policy number (Required for CME credit): _____

**Receipt of CME credit is limited to NORCAL policyholders.*

Target Audience: All providers.

1. Educational Outcomes:

Overall, degree to which the material presented is applicable in your practice setting:

Not applicable | 1 | 2 | 3 | 4 | 5 | *Very applicable*

2. Application of Risk Management Strategies

By providing risk management and patient safety-based strategies, this CME activity is designed to reduce your risk exposure associated with the implementation and utilization of an EHR system. To demonstrate your ability to apply or utilize the risk management recommendations herein, please select the strategies you plan to implement or currently utilize in your practice (mark the box "yes" or "no" for each):

Risk Management Strategies	Yes	No
Ensure you/your staff members and clinicians are aware of and abide by EHR policies and procedures.		
In email exchanges with patients and other providers, utilize proper grammar and punctuation and avoid language that is not considered appropriate within physician/patient communications.		
Remain vigilant regarding patient follow-up; do not rely solely upon EHR features.		
Review records for accuracy, paying special attention to possible errors related to auto-populate features.		
Work with your EHR vendor to design an alert system that is meaningful, and one that minimizes inappropriate or false alerts that might condition users to routinely override or ignore warnings.		

3. Other Strategies to Minimize Risk

The October *Claims Rx* focuses on the physician risks associated with the use of an EHR system. Risks that can be associated with the use of an EHR system include: inaccurate data entry; unauthorized access; disregard of warnings; liability via email consultations; inadequate training; and failure to follow up on abnormal lab values. Recognizing that physician users play an integral part in the success of an EHR system, we addressed the risk areas of communication, follow-up and documentation at the provider level. However, system changes that promote quality and risk management must take place as well for the physician behavioral change to continue successfully. For additional information, please visit our Web site at www.norcalmutual.com/cme, or contact the Risk Management Department at (800) 652-1051, ext. 2244.

4. Was this activity free of commercial bias? Yes No

CME Attestation

I attest that I participated in this CME activity and claim _____ credits (use quarter hour increments) of *AMA PRA Category 1 Credit™* up to a maximum of one credit (hour).

Signature _____

Date (mm/dd/yy) _____

You may submit this form online at www.norcalmutual.com/cme. Or you can mail or fax it to:
Attention: Risk Management, NORCAL Mutual Insurance Company, 560 Davis Street, Suite 200,
San Francisco, CA 94111, Fax: (415) 248-3301