Electronic Medical Record and Social Media Malpractice Risks

Electronic Medical Record—Malpractice Risks
The Doctors Company supports the integration of the electronic medical record (EMR) into medical practices and believes it has great potential to advance both the practice of good medicine and patient safety. However, there are always unanticipated consequences when new technologies are adopted—and the EMR is no exception. Real and potential liability risks are beginning to be recognized, and it is important for doctors to become familiar with them.

1. Doctors are responsible for information to which they have reasonable access—and there may be increased access to e-health data from outside the practice that enters the practice EMR or Web site or that is accessed from the practice EMR or Web site, i.e., hospital charts, consultants’ reports, lab results and radiology reports, community medication histories, etc. If patient injury results from a failure to access or make use of available patient information, the doctor may be held liable.

2. E-prescribing is being rapidly adopted, driven by federal financial incentives, and is currently used by approximately 25 percent of office practices. Potential capabilities and benefits include:
   - Most electronic prescriptions are transmitted via a Sure-scripts network (which has data on 200 million insureds) to all chain pharmacies, 60 percent of independent pharmacies, and most insurance formularies.
   - Most electronic health records (EHRs) have an e-prescribing module, which is a required capability under the federal financial incentives for “Meaningful Use” of EHRs.
   - Standalone e-prescribing software is also available at no cost from Allscripts and the National ePrescribing Patient Safety Initiative (NEPSI).
   - Most programs also check for drug interactions, dosage errors, medication allergies, and patient-specific medication factors.
   - Office prescription renewal requests can be synchronized with most e-prescribing systems and with some personal health records.
   - E-prescribing encourages patients to fill prescriptions (currently 20 percent do not) because their prescription is sent to the pharmacy electronically and is ready to be picked up when they arrive.
   - Costs are lowered by flagging generic and “off-formulary” drugs.

However, practices are exposed to community medication histories through e-prescribing. For example, Dr. A renews a medication, and his e-prescribing program sends an alert advising him that the medication could interact with another drug the patient is taking. He has not prescribed that drug, so his office staff will have to contact the patient to identify who has prescribed it, and then Dr. A will have to contact Dr. X to “negotiate” which drug will be discontinued or changed. If failure to take action results in patient injury from a drug interaction, the doctor may be liable.

3. Because of “alert fatigue,” there is a danger that doctors may ignore, override, or disable alerts, warnings, reminders, and embedded practice guidelines. If it can be shown that following an alert or a guideline would have prevented an adverse patient event, the doctor may be found liable for failing to follow it.

4. Doctors may copy information from a prior note or visit and paste it into a new note or visit (known as “cloning”), making changes where appropriate or documenting by exception. This may result in irrelevant over-documentation, and the patient may appear to have more or less complex problems since the prior encounter. By substituting a word processor for the doctor’s thoughtful review and analysis, the narrative documentation of daily events and the patient’s progress may be lost, thereby compromising the record of the patient’s course. The quality of notes and documentation may be further compromised by the use of templates.

5. The computer may become a barrier between the doctor and the patient. When the doctor fills in a computer template, it may divert attention from the patient, limit interactive conversation, and restrict creative thinking. This may de-personalize and weaken the doctor-patient relationship. The computer’s location in the office is an important ergonomic consideration; i.e., the location of electrical outlets shouldn’t force you to sit with your back to the patient.

6. Many EMRs autopopulate fields in the history and physical (H&P) (from data derived from data fields in a prior H&P) and in procedure notes (from personalized or packaged templates). While over-documentation may facilitate billing, entering erroneous or outdated information may increase liability. For example, an internist was deposed, and his EMR was the medical record. Some of the autopopulated fields contained obviously wrong information. At deposition, the plaintiff’s attorney asked these questions:
PATIENT SAFETY/RISK MANAGEMENT ARTICLE

a. “So is the information in this record accurate or not?”

b. “Do you bother looking at your records?”

c. “If these ‘autopopulated’ fields are incorrect, can we trust anything in this record?”

d. “Do you deliver the same level of care as you do in record keeping?”

7. “Meaningful Use” requires online patient connectivity. Some EMRs have patient questionnaires that use an algorithm to interview the patient. These questionnaires often address—and memorialize in the record—issues that many doctors are simply not prepared to pursue (depression, substance abuse, etc.). Lack of or incomplete follow-up can create potential liability—and provide a clear record for the plaintiff’s attorney to follow.

8. Vendor contracts may attempt to shift medical liability risks resulting from faulty software design or decision support data onto the doctor. They may also provide that the vendor has rights to utilize patient or provider data. Read all contracts carefully.

9. Electronic discovery: Lawyers may request not only printed copies of the EMR but also the raw e-data for metadata analysis. This includes logon and logoff times, what was reviewed and for how long, what changes or additions were made, and when the changes were made. Smart phone and e-mail records are also discoverable. Doctors need to know that all of their interactions with the EMR are time-tracked and discoverable.

10. Templates with drop down menus facilitate data entry. However, drop down menus are usually integrated with other automated features. An entry error may be perpetuated elsewhere in the EMR—and it may be overlooked, resulting in a new potential for error. Erroneous information, once entered into the EMR, is easily perpetuated and disseminated.

11. Many EMRs provide e-prescribing drug information and clinical decision support, and the government’s “Meaningful Use” requirements mandate minimum functionalities in both of these areas. Clinicians should know the source of drug and clinical decision support information in their EMRs, because they may be held accountable to the clinical standards of care for their specialty and for the information in FDA-approved drug labels or drug alerts.

Social Media—Malpractice Risks

Social media (YouTube, Twitter, Facebook, MySpace, blogs, etc.) are used by doctors for doctor-to-doctor networking. However, these types of media are not appropriate for doctor-patient communications because they are too informal and lack an atmosphere of professionalism—making it easy to lapse into casual conversation and inadvertently cross the boundary between personal and professional relationships. The following recommendations are made regarding the use of social media:

1. Do not discuss individual patients, dispense medical advice, respond to clinical questions from patients, or otherwise practice medicine on these sites. These types of media do not use HIPAA-compliant secure networks, and inadvertently disclosing a patient’s health information will violate HIPAA.

2. Presume that anything you say or post is in the public domain, and remember that anything typed or e-mailed creates a permanent record that is subject to discovery.

3. Doctor office practices should have written confidentiality and communication policies with employees that clearly forbid online disclosure or discussion of patient health information.

This article originally appeared in The Doctor’s Advocate, third quarter 2010, www.thedoctors.com/advocate.

By David B. Troxel, MD, Medical Director, Board of Governors.

Founded by doctors for doctors in 1976 to advance, protect, and reward the practice of good medicine, The Doctors Company is the largest national insurer of physician and surgeon medical liability. For more information on our innovative patient safety products and services, please call (800) 421-2368, extension 1243, or visit us at www.thedoctors.com/patientsafety.

The guidelines suggested here are not rules, do not constitute legal advice, and do not ensure a successful outcome. The ultimate decision regarding the appropriateness of any treatment must be made by each health care provider in light of all circumstances prevailing in the individual situation and in accordance with the laws of the jurisdiction in which the care is rendered.