Medical Malpractice

Litigation in the Decade of Electronic Health Records

Use of EHRs may raise new risks of malpractice liability

By Joel B. Korin and Madelyn S. Quattrone

In years to come, the paper hospital record will be viewed as a historical curiosity. Electronic health information technology (IT) is transforming the delivery of health care in the United States. The Institute of Medicine’s (IOM) 2001 report, *Crossing the Quality Chasm: A New Health System for the 21st Century* recognizes that IT must play a central role in the redesign of the health-care system to support improvements in quality and patient safety. IOM envisions health-care records that are created and stored electronically and that are transmissible through an electronic network serving as the foundation for a comprehensive health IT system. Key capabilities would include clinical documentation, health information, results management, order-entry management, clinical decision support, electronic communication and connectivity, patient support, administrative processes, reporting and disease surveillance.

In 2004, President George W. Bush, calling for an electronic health record (EHR) for most Americans by 2014, established a new office within the U.S. Department of Health and Human Services (HHS) — the Office of the National Coordinator for Health Information Technology — to coordinate and promote health IT. The office identified four goals to guide the adoption of IT in the nation’s private and public healthcare sectors: 1) the adoption of EHRs; 2) the development of a secure national health information network to permit the exchange of health information among clinicians; 3) the use of personal health records by patients; and 4) the improvement of public health through quality measurement, research and dissemination of evidence.

With EHRs, clinicians’ notes may be entered in text or standard formats, fostering more complete documentation; radiology images may be captured from computerized picture archiving systems and wave forms, such as electronic fetal monitoring, may be transmitted to clinicians in remote locations; computerized prescriber order-entry systems (CPOEs) allow physicians to order laboratory, pharmacy, and radiology services electronically, thus reducing the time for delivery of medical services and improving communication among providers. EHRs may provide users with electronic reminders, alerts to medication allergies or medication contraindications, access to protocols, clinical guidelines and the like.

But reports of adverse events associated with the use of EHRs are coming to light as hospitals increasingly adopt electronic IT system applications. For example, a pediatric health-care facility reported an increase in mortality among critically ill children after the installation of a commercially available CPOE system reportedly required physicians and nurses to use time previously spent at patients’ bedsides in front of computer screens. Han Y., Carcillo J., Vankataraman S., et al. “Unexpected Increased Mortality After Implementation of a Commercially Sold Computerized Physician Order Entry System.” *Pediatrics* 2005 Dec; 116(6):1506-12. Problems encountered during the effort by a large California health maintenance organization to digitize its system involving 12,000 physicians, more than 400 medical offices, 36 hospitals in nine states, and millions of patients have been reported. Costello D., “Kaiser Has Aches, Pains Going Digital” *L.A. Times* (online), Feb. 15, 2007. During a nine-month period in which the EHR system experienced power outages, nearly two dozen incidents of system unreliability were
thought to have caused risk to patient safety.

Although use of EHRs is integrally related to improving patient safety, adopting EHRs may raise new risks of malpractice liability. Data loss or destruction, inappropriate corrections to the medical record, inaccurate data entry, unauthorized access, and errors related to problems that arise during the transition to EHRs are potential liability issues. These concerns are not unique to EHRs — the same concerns exist with regard to paper medical records.

Hospitals will likely adopt policies and procedures that are feasible and compatible with EHR system functionalities and address areas of potential risk. For example, the EHR system should provide a clear record of when a correction or addition is made in accordance with facility policy. The integrity, accessibility, security, and privacy of protected health information must be addressed through policies and procedures that support the requirements of the Health Insurance Portability and Accountability Act’s security and privacy regulations. EHR systems may have built-in safeguards to flag certain kinds of data entry errors and to prevent inadvertent data loss.

EHRs will make voluminous patient data available to clinicians. Will physicians have a legal duty to access patients’ past medical records? Historically, the duty to obtain and consult a patient’s past medical record has been adjudicated on a case-by-case basis, requiring medical expert-witness opinion testimony concerning whether the standard of care required the defendant physician to take such action. As EHRs are adopted and increasingly integrated into established regional networks, or a national network, the standard of accepted practice will evolve.

Exercising clinical judgment, physicians may decide to override an electronic alert concerning a specific medication or choose a course of action that is not contemplated in a clinical guideline provided in the EHR system. A CPOE system that requires users to document reasons for clinical overrides may generate documentary evidence, which can serve as a sword or a shield if the decision to override is questioned in a malpractice case or in peer-review proceedings. Will the standard of care be shaped by a software vendor’s choice of clinical-decision-making tools? Might software vendors or software manufacturers routinely become co-defendants and/or witnesses in medical negligence lawsuits? Will greater weight be assigned to electronically generated guidelines that are built into system software created by a healthcare institution rather than provided by a commercial vendor? Can a physician successfully assert a defense that “alert fatigue” caused her to override an alert because the system routinely provides overrides that clinicians view as inappropriate?

Because more detailed information about patient care or medical decision-making may be included in the EHR than is possible with paper records, plaintiff attorneys may make extensive discovery requests for “relevant” electronic information in medical malpractice litigation. For example, integrated EHRs have the capability to create an electronic traceable path of a patient’s transition through a facility. Physician orders and interventions may be timed and documented automatically. Will such functionality increase the risk of liability in cases alleging physician failure to timely diagnose and treat? Will discovery requests include electronic footprints for relevant patient data that is not part of the facility’s permanent electronic medical records? Will use of EHRs raise the cost of litigation because of the need for expert testimony in the fields of health informatics or health IT?

Sweeping amendments to the Federal Rules of Civil Procedure will impact discovery of electronic health information in malpractice cases. Effective December 2006, the rules mandate that counsel assess very early in the case how digital information is stored, how it can be produced for the adversary party, and what kind of electronic evidence is relevant to the claims and defenses asserted. Unless otherwise privileged from discovery, all electronically stored information that the disclosing party may use to support its claims or defenses, must be disclosed. Notably, discoverable electronic information may include data that has not traditionally been considered by the hospital to be part of the patient’s health record. Day, S., E-Discovery: Practical Tips for E-Survival, remarks at the Meeting of the Philadelphia Area Society for Healthcare Risk Management; Jan. 25, 2007; ECRI Institute, Plymouth Meeting (PA).

Although most medical negligence cases are filed in state courts, and thus not governed by federal procedure rules, state court rules will likely be amended to specifically address electronic discovery. New Jersey, for example, adopted electronic discovery rules mirroring the federal rules.

To meet discovery challenges, attorneys will need to become familiar with systems and processes that are used to create, transmit and store health care information electronically; what electronic information is available; how routine computer operations in health care institutions may change or alter electronically stored data; and what is entailed in producing requested electronic documents. Information that is relevant to a medical negligence lawsuit, for instance, may be stored electronically in e-mails, a health care provider’s Web pages, word-processing files and databases stored in electronic memory systems, such as magnetic disks (e.g., computer hard drives), optical disks (e.g., DVDs, CDs), and flash memory (e.g., “thumb” or “flash” drives). An electronic document thought to be “lost” or deleted might be recoverable from a computer’s hard drive and may be available from other computers, including physicians’ home computers, and on archival media or backup tapes used for disaster recovery that may be managed and stored off-site.

Electronic discovery may also involve metadata or embedded electronic data that is typically “hidden” from view of computer users in ordinary circumstances. Metadata provides information about an electronic document, such as the date it was created, its author,
when and whom it was edited, what edits were made, and, for e-mail, the history of its transmissions. Embedded data includes commands that control or manipulate data, such as computation formulas or word-processing formatting commands. Metadata is discoverable under the federal electronic discovery rules, but courts will have to decide when and how it can be used on a case-by-case basis. The discovery rules may require that metadata created by CPOEs be produced, even in situations for which hospital policy does not require the data to be integrated into a patient’s permanent health record. Day, S., E-Discovery: Practical Tips for E-Survival, remarks at the Meeting of the Philadelphia Area Society for Healthcare Risk Management; Jan. 25, 2007; ECRI Institute, Plymouth Meeting (PA). For example, pursuant to hospital policy, the EHR system does not integrate clinical overrides made in ordering medication through CPOE systems into the HER. Rollins G. “The Prompt, the Alert, and the Legal Record: Documenting Clinical Decision Support Systems,” J AHIMA 2005 Feb; 76(2):24-8. Although the override is not captured in the EHR, the computer system may make the data retrievable, consequently bringing to light in discovery a physician’s apparent thought process at the time the override was made.