IT Vendor and Institutional Liability for Electronic Health Records

Ronald L. Scott
rscott@central.uh.edu

Assume that a physician relies on health information contained in a patient’s electronic health record (EHR) shared electronically from another provider. However, the wrong information has been associated with the patient by the information system, and injury occurs. Is the information technology (IT) vendor liable? What exposure does the hospital or other health care system responsible for maintaining the EHR have?

Designers of systems allowing shared access to EHRs incorporate protections to help prevent errors in association of medical information with a particular patient. For example, the Santa Barbara County Care Data Exchange (SBCCDE)\(^1\) (a clinical data exchange system) incorporates an “identification correlation process” to help prevent such errors.\(^2\) However, “the designers of the identification correlation process…admit it is not perfect and could conceivably result in a misidentification of the proper patient receiving treatment.”\(^3\) The SBCCDE and other systems require participants to accept a contractual provision limiting liability for errors in the electronic data.\(^4\) Advocates of shared systems point out that patient misidentification can occur in paper as well as electronic systems and that electronic systems have features more likely to prevent such errors.\(^5\) Further, legal issues arising from such errors “are not substantially different when the medical record system is a paper one.”\(^6\)

It is highly unlikely that an information technology (IT) vendor would end up with significant liability if a software error resulted in patient misidentification because IT vendors ordinarily shift liability risks to users contractually.\(^7\) In a breakout session held at the American Health Lawyers Association’s 2003 Public Interest Colloquium (discussing legal issues relating to the use IT in reducing medical errors),\(^8\) participants “agreed that vendors should be held accountable for the performance of their products.”\(^9\) Participants suggested that economic incentives could lead to increased product reliability and facilitate vendor’s assuming more responsibility for product performance.\(^10\)

\(^3\) Id.
\(^4\) Id.
\(^5\) Id.
\(^6\) Id.
\(^7\) Elizabeth Belmont and Adele A Waller, The Role of Information Technology in Reducing Medical Errors, 36 J. HEALTH L. 615, 620-21 (2003).
\(^8\) Id. at 615.
\(^9\) Id. at 621.
\(^10\) Id.
Additionally, providers could demand that vendors assume more responsibility or “be subject to market discipline.”\textsuperscript{11} The participants were not in favor of state regulation of IT because such regulation could result in “state-by-state differences and conflicts in laws and regulations.”\textsuperscript{12}

Institutions such as hospitals and managed care organizations that operate and maintain EHR systems could be held liable for damages suffered by a patient under a theory of “corporate liability.”\textsuperscript{13} Corporate liability may attach where the “structure of the health services themselves proximately causes injury.”\textsuperscript{14} A common example of corporate liable is where a hospital or managed care organization is held liable for “negligent credentialing.” For example, an HMO that contracts with an unlicensed physician “can be held liable for sending patients to that individual for treatment.”\textsuperscript{15} Using a theory of corporate liability, an injured patient could hold a hospital responsible where the hospital provided physicians with a substandard medical record system and the patient suffered injury because of such medical record system.

In Texas, \textit{public} hospitals may be able to invoke principles of sovereign immunity to avoid liability for negligence unless sovereign immunity is waived pursuant to statute. In \textit{University of Texas Medical Branch [UTMB] at Galveston v. York} the court considered “whether the use, misuse, or nonuse of information which is recorded in a patient’s medical records is a use of tangible personal property under...the Texas Tort Claims Act [TTCA],...and thus satisfies a condition for waiver of governmental immunity.”\textsuperscript{16} The court rendered judgment in favor of UTMB, holding that “while paper itself can be touched, handled, and seen, medical information recorded on paper is not tangible personal property,”\textsuperscript{17} and the state has therefore not waived immunity from liability.\textsuperscript{18} The court noted that York did not allege misuse of a hospital device or equipment, which could have resulted in a waiver of liability under the TTCA.\textsuperscript{19} Rather, York alleged that UTMB misused tangible personal property by failing to record certain events and observations in the medical record and by further failing to rely on information that was recorded.\textsuperscript{20} This case involved paper rather than electronic medical records, so a future plaintiff could seek to distinguish this holding by arguing that the computer system used to maintain medical records is a “hospital device or equipment.” However, in this case the court accepted that the paper used to record medical information is tangible personal property, since it can be seen and touched, but said that “information itself is an abstract concept, lacking corporeal, physical, or palpable qualities. Information thus, is intangible;

\begin{itemize}
\item \textsuperscript{11} Id.
\item \textsuperscript{12} Id.
\item \textsuperscript{13} Id.
\item \textsuperscript{14} Id.
\item \textsuperscript{15} Id. Under Texas law, negligent credentialing claims “involve a claimed departure from an accepted standard of health care.” Garland Community Hospital v. Rose, 156 S.W.3d 541, 546 (Tex. 2004).
\item \textsuperscript{16} Univ. of Tex. Med. Branch v. York, 871 S.W.2d 175 (Tex. 1994)
\item \textsuperscript{17} Id.
\item \textsuperscript{18} Id.
\item \textsuperscript{19} Id. at 178.
\item \textsuperscript{20} Id.
the fact that information is recorded in writing does not render the information tangible property.\textsuperscript{21} Therefore a future court could find the computer hardware used in an electronic medical record system to be tangible personal property but the information contained therein to be intangible, retaining the public hospital’s sovereign immunity defense.

Institutional providers such as hospitals and other healthcare facilities must also comply with medical records requirements required for accreditation and for eligibility to participate in governmental programs such as Medicare and Medicaid.\textsuperscript{22} Such institutional providers risk “loss of licensure, accreditation, and eligibility to participate in federal healthcare programs.”\textsuperscript{23} Therefore, from both a regulatory and a risk management standpoint, hospitals, managed care organizations and other healthcare institutions have strong incentives to maintain accurate medical records, whether in paper or electronic form.

The legal issues associated with paper and electronic records in this context are very similar, so from a risk management standpoint the hospital would need to consider whether patient misidentification is more or less likely to occur with an electronic system compared to a paper system. At present, any incremental risks associated with “computer error” appear theoretical. It seems unlikely that market forces will compel IT vendors to assume malpractice liability exposure, but shared EHRs may help reduce medical error and therefore malpractice exposure. Therefore risk management issues will hopefully not present a significant barrier to the adoption of shared EHRs.

August 2006

\textsuperscript{21} Id.

\textsuperscript{22} WILLIAM H ROACH ET. AL., MEDICAL RECORDS AND THE LAW 52 (4th ed. 2006).

\textsuperscript{23} Id.