E-Health and Oncology: A Legal Perspective

by J. Peter Rich, J.D., and Scott A. Edelstein, J.D., M.P.A.

For many health care providers, e-health via the Internet and other cyber tools may represent both an alternate source of revenue and a more cost-effective means of health care delivery. Unfortunately, to stay financially afloat in these difficult economic times, a number of providers are taking legal risks of which they may be unaware. Here are a few examples taken from real-life transactions:

- An oncology practice's marketing plan promotes a supplier's products via the Internet. The practice is expected to refer patients to the supplier's web site in exchange for a percentage of the price of the products sold.
- A pharmaceutical firm enters into an arrangement with an oncologist who provides a list of all patients who have recently been prescribed one of its drugs.
- An oncologist in an e-health network subsidizes the network's costs, while other physicians in the same network routinely refer patients to that oncologist.
- An oncologist sets up a web site to provide advice to Internet users about their illnesses and allows other oncologists to be listed on the web site for a fee.
- A group of oncologists forms a general business corporation to contract with physicians in other states to provide teleconsultations.

Each of these situations could involve legal violations, depending on the types of services involved and the precise terms of the transaction (such as the ways in which the participants are compensated, the precise method in which the transaction is structured, the regulatory or other legal framework under which they arise, and the type of reimbursement available for the applicable health care services). Determining whether a practitioner's conduct is legal or not requires a thorough and often complex legal analysis of each of these factors. Before you contemplate developing or participating in an e-health enterprise, having at least a basic understanding of these issues will help to lessen your legal risks.

J. Peter Rich, J.D., and Scott A. Edelstein, J.D., M.P.A., are partners in the Los Angeles office of the international law firm of McDermott, Will & Emery.

PATIENT CONFIDENTIALITY AND PRIVACY

As practitioners increasingly use technology to transmit medical records, perform image transfers, and conduct electronically assisted consultations, questions of patient privacy and confidentiality arise. The potential for interception and misappropriation of confidential patient information can be significant. A typical patient's medical record may be viewed by dozens of people, including a clinical laboratory, employee wellness program, retail pharmacy, managed care organization, and accrediting organization.

To alleviate this concern, federal and state laws have established standards for the maintenance of patient medical records and protocols to protect the confidentiality of individual patient information, whether in electronic form or otherwise. Unfortunately, there is little consistency in this patchwork of state laws, which presents a significant challenge for interstate e-health providers.

The federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) seeks to safeguard the privacy of individually identifiable health information by regulating its use and disclosure. Except for certain limited exceptions, HIPAA prohibits the disclosure of patient-identifiable information to a third-party for reasons unrelated to payment, treatment, or health care operations unless the patient's express written authorization has been obtained. Under recently published privacy regulations interpreting HIPAA, oncologists and other health care providers will have until April 14, 2003, to establish policies and procedures to comply with the privacy requirements. A violation of these regulations could result in significant monetary penalties and even imprisonment.

In addition, the Centers for Medicare and Medicaid Services (CMS, formerly the Health Care Financing Administration) issued guidelines governing the Internet transmission of patient-identifiable information for Medicare patients. The new policy permits CMS staff, contractors, and subcontractors to use the Internet for "sensitive data" if appropriate encryption, authentication, and identification procedures are used. Many observers have hailed the new policy because it revised the agency's longstanding prohibition against using the Internet to transmit certain CMS data.

MALPRACTICE

Oncologists need to know whether their malpractice insurance policies cover e-health services, and if so, whether such coverage applies to services provided to patients located outside the practitioner's state or country. Teleconsultation networks that cross state or international boundaries create additional

uncertainties about the jurisdiction where a malpractice lawsuit may be litigated and the laws that may apply. Jurisdictions have different statutes of limitation and, more importantly, different statutory limits placed on the amount of malpractice awards. Depending on how the e-health venture is structured and the jurisdiction(s) in which it is located, there is the potential for vicarious or corporate liability for a teleconsultant's malfeasance. Therefore, it is essential that professionals providing medical services through an e-health network have sufficient malpractice coverage.

In a teleconsultation, questions also arise concerning which standard of care should be applied in malpractice suits. For example, if the community standard of care is upheld, which community standard applies—that of the rural community where the referring practitioner is located or the urban community where the consulting practitioner is located? Because e-health practitioners could practice nationwide, a good argument can be made that a national standard of care should apply. The recent establishment of a web-based repository for clinical practice guidelines by the Agency for Health Care Policy Research (AHCPR) (see http://www.guideline.gov) will likely bolster this argument.

Malpractice carriers are divided on the issue of whether providers should maintain a videotaped record of telemedicine encounters. Videotapes can be a double-edged sword. On the one hand, a videotape can assist in the defense of a malpractice case if it demonstrates that the provider met the appropriate standard of care. On the other hand, if the provider arguably deviated from that standard of care, a videotape can powerfully support the plaintiff's case.

Another issue is whether an e-health encounter creates a physician-patient relationship. Such a determination may be difficult when a patient does not have direct contact with the consulting practitioner. For example, if an oncologist reviews a patient's medical record, that review could be deemed either an informal consultation between two colleagues or the establishment of a formal physician-patient relationship. Unfortunately, the answer is uncertain due to the lack of professional guidelines and clear legal precedent.

A WEB OF LEGAL CONCERNS

In addition to patient confidentiality and malpractice issues, there are several other legal issues to ponder.

Informed consent. Standard informed consent principles require a physician to provide enough information to the patient to allow the patient to make an informed decision about both his or her diagnosis and treatment. If remote consulting is an integral part of the care being provided, it may be necessary to disclose information about the e-health system, the potential risks and benefits of e-health, and the limitations of the equipment and telecommunications technology. The physician who has ultimate responsibility for care and primary diagnosis should obtain the patient's oral and written informed consent prior to an e-health encounter.

Licensure and credentialing. Although many e-health interactions are already crossing state and national boundaries, legal precedents for remote professional licensure are not yet established. Currently, physicians and other health care practitioners must satisfy numerous requirements to obtain a license to practice medicine in each state and be credentialed to practice at each health care facility. The Federation of State Medical Boards (FSMB) has proposed that licensure and certification requirements be standardized to allow practitioners to perform services across state lines without having to undergo re-examination and/or refile fees. The FSMB has drafted model legislation to facilitate the practice of telemedicine across state lines; however, several states have enacted legislation requiring full and unrestricted state licensure of out-of-state health care providers. An oncologist interested in providing advice via the Internet to consumers should be cautious about whether such advice constitutes the practice of medicine in the state where the consumer is located, and therefore might unwittingly cause the oncologist to be subject to the state's medical practice laws.

Some jurisdictions have informally indicated that the establishment of a telemedicine presence may even be considered a new health service subject to the jurisdiction's certificate of need and/or facility licensing laws. Before establishing a telemedicine presence in a state, applicable state law should be reviewed, and, if necessary, the local health planning department should be consulted.

Managed care regulation. E-health entrepreneurs have set up physician networks similar to preferred provider organizations (PPOs), and then have offered a "medical access card" for sale on their web site. These cards, which are generally sold for a nominal amount such as $25 per year, entitle the purchaser to receive discounted rates from the company's provider panel. Since these cards are not offered by or through licensed health insurers or HMOs, and are not offered under a self-funded ERISA plan governed by the U.S. Department of Labor, they may run afoul of state insurance/HMO laws (as well as the corporate practice of medicine as discussed below). For example, over the past two years the California Department of Managed Health Care (CDMHC) has taken a particularly aggressive regulatory posture with respect to such health programs, devoting the time of at least one of its attorneys to "surfing the net" to uncover web sites that target California consumers. Numerous such web sites had been forced by the California regulators to cease offering their programs to California residents. However, on June 7, 2001, the director of the CDMHC reversed this position and declared that these programs were outside its jurisdiction and therefore regulated only by applicable consumer protection laws. While California often sets regulatory trends for the country, each state's insurance and HMO regulations should be considered when health benefits programs are offered to that state's residents.

Corporate practice of medicine and fee splitting. E-health networks are frequently owned and/or operated by a separate legal entity that does not hold a medical, insurance, or HMO license and that contracts with physicians to provide teleconsultations. This arrangement could

be problematic in the many states where the practice of medicine or professional "fee splitting" by either unlicensed individuals or non-medical corporations is prohibited. The rationale behind these prohibitions is to prevent physicians and non-physicians from engaging in financial relationships that could adversely affect the quality of medical care. Some states provide limited exceptions to this prohibition for HMOs, professional corporations, and hospitals. E-health ventures must be structured carefully to avoid such corporate practice and fee-splitting prohibitions.

Fraud and abuse/self referral. Any financial arrangement among practitioners in an e-health network may raise issues under federal and state antifraud and abuse and self-referral laws, particularly because network participants, due to their technological ties, may be tempted to refer patients to each other. For example, if an oncologist in a teleconsulting network subsidizes the network's capital and/or operating costs and other physicians in the network refer patients to that oncologist, state and federal agencies may conclude that such subsidies were intended to lock in a referral stream. In addition, many states prohibit physicians from receiving a commission in exchange for referring patients, and at least one state has determined that such an Internet marketing arrangement is prohibited.

Franchise laws. Franchise laws require the registration of arrangements under which one party (the "franchisor") requires another party (the "franchisee") to 1) adhere to the franchisor's marketing plan, 2) license use of the franchisor's trade name to the franchisee, and 3) collect a fee in return. Whether the parties refer to themselves as "franchisors" or "franchisees," the failure to register an arrangement that meets those three elements may subject the franchisor to thousands of dollars in daily fines. Some health entrepreneurs have attempted to interest physicians in becoming unwitting "franchisees" under such an arrangement, though the entrepreneur has never registered as a franchisor.

Intellectual property. Much e-health technology is subject to restrictions based on intellectual property law. For example, computer software and other original works of authorship "fixed in a tangible medium of expression" are protected by federal copyright law. Equipment used in e-health systems may be subject to patents. Even business processes may now be patented, and other aspects of an e-health system may be protected as trade secrets under state law.

> ...an unlawful price-fixing arrangement may arise if oncologists in an e-health network reveal financial or charge data to one another directly or indirectly.

Antitrust. Providers must be especially cognizant of the antitrust or price-fixing risks of database structure and usage, especially if anticompetitive risks arise from its use. For example, an unlawful price-fixing arrangement may arise if oncologists in an e-health network reveal financial or charge data to one another directly or indirectly.

Electronic prescribing. Technological advances now allow physicians to prescribe medication electronically via e-mail from a prescriber to a pharmacy or via electronic submission from a prescriber's hand-held device to a pharmacy. Some states do not allow prescriptions via electronic means, and those that do permit electronic prescriptions may not do so for certain controlled substances. The recent enactment of the Electronic Signatures in Global and National Commerce Act, which gives electronic signatures the same legal significance as inked signatures, should help further the expansion of this aspect of the e-health industry.

The Drug Enforcement Agency and many state pharmacy boards are in the process of reviewing existing prescription guidelines to address electronic prescriptions. Recently, the Federal Trade Commission launched Operation "Cure.all," a comprehensive law enforcement and consumer education campaign targeting Internet health fraud, and several states have taken legal action against fraudulent online pharmacies.

Medical device regulation. Certain e-health software and hardware are subject to the Food and Drug Administration (FDA) approval process. The FDA's Center for Devices and Radiological Health recently established guidelines for regulation of telemedicine devices. As the FDA's regulation of e-health devices grows, providers are advised to consult with appropriate counsel prior to marketing new e-health technology.

ETHICAL GUIDELINES

In addition to legal issues, ethical quandaries have developed for e-health providers, including determining when a physician/patient relationship is established, whether a remote examination can be substituted for an in-person examination, the quality of the content on a web site, the possibility that advertising and sponsorship will improperly influence content, and the possibility that personal privacy and confidentiality will not be preserved.

Several voluntary ethical organizations have emerged to address these issues (e.g., Health on the Net, Hi-Ethics). The American Medical Association recently created guidelines for AMA web sites, which the AMA believes could also be used to provide guidance for the creators of other web sites that provide medical and health information for professionals and consumers. The guidelines are intended to alleviate consumer concerns and monitor health care provider conduct relating to the security of electronic financial transactions, privacy and confidentiality of patient medical information, and advertising content on the site.

While many e-health practitioners have found the legal issues and uncertain regulatory environment daunting, some of the issues have relatively straightforward solutions. With careful planning, oncologists and other e-health providers can greatly reduce their legal exposure.